Copyright 2005-2007 ValuePoint Networks, Inc. All rights reserved.

SuperAP™ Rugged Access Points/Bridges

500 Series

802.11b Models

500, 500DR
500IA-12, 500IA-18, 500IA-12DR

802.11b/g Models

510g, 510gDR, 510g 500MW
530g, 550g, 570g
530gIA-12, 530gIA-18, 550gIA-12

User's Guide

December 4, 2006

Copyright 2005-2007 ValuePoint Networks, Inc. All rights reserved.

Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiated radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

FCC Caution: To assure continued compliance, (example – use only shielded interface cables when connecting to computer or peripheral devices). Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

FCC Radiation Exposure Statement

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20 cm between the radiator & your body.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Copyright 2005-2007 ValuePoint Networks, Inc. All rights reserved.

R&TTE Compliance Statement

This equipment complies with all the requirements of DIRECTIVE 1999/5/CE OF THE EUROPEAN PARLIAMENT AND THE COUNCIL OF 9 March 1999 on radio equipment and telecommunication terminal equipment and the mutual recognition of their conformity (R&TTE).

The R&TTE Directive repeals and replaces in the directive 98/13/EEC (Telecommunications Terminal Equipment and Satellite Earth Station Equipment) as of April 8,2000.

Safety

This equipment is designed with the utmost care for the safety of those who install and use it. However, special attention must be paid to the dangers of electric shock and static electricity when working with electrical equipment. All guidelines of this and of the computer manufacture must therefore be allowed at all times to ensure the safe use of the equipment.

EU Countries Intended for Use

The ETSI version of this device is intended for home and office use in Austria, Belgium, Denmark, Finland, France (with Frequency channel restrictions), Germany, Greece, Ireland, Italy, Luxembourg, Portugal, Spain, Sweden, The Netherlands, and United Kingdom.

The ETSI version of this device is also authorized for use in EFTA member states Norway and Switzerland.

EU Countries Not Intended for Use

None.

Potential Restrictive Use

France: only channels 10, 11, 12, and 13.

Copyright 2005-2007 ValuePoint Networks, Inc. All rights reserved.

Table of Contents

1. Introduction 1
    1.1. Overview 1
    1.2. Features 1
2. First-Time Installation and Configuration 5
    2.1. Selecting a Power Supply Method 5
    2.2. Mounting the AP on a Wall 5
    2.3. Connecting Antennas 6
    2.4. Preparing for Configuration 6
        2.4.1. Connecting the Managing Computer and the AP 6
        2.4.2. Changing the TCP/IP Settings of the Managing Computer 7
    2.5. Configuring the AP 7
        2.5.1. Step 1: Selecting an Operational Mode 8
        2.5.2. Step 2: Configuring TCP/IP Settings 9
        2.5.3. Step 3: Configuring IEEE 802.11 Settings 10
        2.5.4. Step 4: Reviewing and Applying Settings 11
    2.6. Deploying the AP 11
    2.7. Setting up Client Computers 12
        2.7.1. Configuring IEEE 802.11-Related Settings 12
        2.7.2. Configuring TCP/IP-Related Settings 13
    2.8. Confirming the Settings of the AP and Client Computers 13
        2.8.1. Checking if the IEEE 802.11-Related Settings Work 13
        2.8.2. Checking if the TCP/IP-Related Settings Work 13
    2.9. Resetting the Access Point to Factory Default 14
3. Using The Web-Based Network Manager 15
    3.2. AP Status 17
        3.2.1. Associated Wireless Clients 17
        3.2.2. Current DHCP Mappings 18
        3.2.3. System Log 18
        3.2.4. Link Monitor 19
    3.3. General Operations 19
        3.3.1. Specifying Operational Mode 19
        3.3.2. Changing Password 22
        3.3.3. Managing Firmware 22
    3.4. Configuring TCP/IP Related Settings 26
        3.4.1. Addressing 26
        3.4.2. DHCP Server 26
    3.5. Configuring IEEE 802.11-Related Settings 27
        3.5.1. Communication 27
        3.5.2. Security 33
        3.5.3. IEEE 802.1x/RADIUS (Adv+ and DR only) 38
    3.6. Configuring Advanced Settings 39
        3.6.1. Packet Filters 39
        3.6.2. Management 41
Appendix A: Default Settings 43
Appendix B: Troubleshooting 44
    B-1: Wireless Settings Problems 44
    B-2: TCP/IP Settings Problems 45
    B-3: Other Problems 46
    B-3: Contacting Technical Support 47
Appendix C: Additional Information 48
    C-1: Distances and Data Rates for Clients 48

Copyright 2005-2007 ValuePoint Networks, Inc. All rights reserved.

1. Introduction

1.1. Overview

The SuperAP™ Rugged Access Point/Bridge 500 Series (AP) enables IEEE 802.11b/g client computers to access the resources on the network infrastructure. The Rugged Access Point is housed in a durable hardened enclosure that is tamper resistant, which makes the AP perfect for public deployments indoors or outside. With the Web-based user interface a network administrator can easily and clearly manage the AP.

The SuperAP DR (Dual Radio) versions are multi-function devices that have two independently configurable RF interfaces. Each RF interface can be configured either as an AP (Access Point) interface or a LAN-to-LAN bridge interface. An AP interface enables wireless clients to associate with this device for IEEE 802.11 infrastructure applications and the wireless clients can be authenticated by IEEE 802.1x/RADIUS (with optional upgrade). A LAN-to-LAN bridge interface enables the device to connect to up to 6 other bridges wirelessly by the Wireless Distribution System (WDS) technology.

The SuperAP (Integrated Antenna) IA versions include an integrated 12dbi or 18dbi directional antenna integrated and sealed with the SuperAP hardware.

In Chapter 2, we describe the steps to install and configure a newly acquired AP. Following the steps, the AP can be quickly set up. In Chapter 3, detailed explanations of each Web management page are given for the user to understand how to fine-tune the settings of an AP to meet his or her specific needs.

NOTE: By convention, documentation referencing the 'AP' describes all models, unless there is an explicit exception. Documentation referencing the 'DR' describes the Dual Radio only.

WARNING: The high-power radio in this Access Point requires an attached antenna to function correctly. Running the Access Point with no antenna may damage the radio and reduce maximum radio power.

1.2. Features

- **IEEE 802.11**
  - **Operational modes**
    - **AP/Bridge ("AP Repeater" on DR).** This mode provides both Access Point and *Static* LAN-to-LAN Bridging functionality. The static LAN-to-LAN bridging function is supported through Wireless Distribution System (WDS).
    - **AP Client (Not available on DR).** This mode is for *Dynamic* LAN-to-LAN Bridging. The AP Client automatically establishes bridge links with APs from any vendors.

Copyright 2005-2007 ValuePoint Networks, Inc. All rights reserved.

- **Dual AP (DR only).** This mode provides two independent wireless networks that can be configured with different SSIDS and channels. Each network has a dedicated radio attached to a separate antenna.

- **Bridge Repeater (DR only).** In this mode, both WLAN interfaces are configured as LAN-to-LAN bridge interfaces. A bridge repeater forwards packets between two wireless LAN-to-LAN bridges. It's possible to use multiple bridge repeaters in between two LAN-to-LAN bridges to span long distances.

- **64-bit and 128-bit WEP (Wired Equivalent Privacy).** For authentication and data encryption.

- **WPA (Wi-Fi Protected Access)** The AP supports the WPA standard proposed by the Wi-Fi Alliance (http://www.wi-fi.org). Both WPA-PSK (Pre-Shared Key) mode and full WPA mode are supported. WPA is composed of TKIP (Temporal Key Integrity Protocol) and IEEE 802.1x and serves as a successor to WEP for better WLAN security.

- **Enabling/disabling SSID broadcasts.** When the AP is in AP/Bridge mode, the administrator can enable or disable the SSID (Service Set ID) broadcasts functionality for security reasons. When the SSID broadcasts functionality is disabled, a client computer cannot connect to the AP with an "any" network name SSID or select the SSID from a list; the correct SSID has to be specified on client computers.

- **MAC-address-based access control.** When the AP is in AP/Bridge mode, it can be configured to block unauthorized wireless client computers based on MAC (Media Access Control) addresses. The ACL (Access Control List) can be downloaded from a TFTP server.

- **IEEE 802.1x/RADIUS** When the AP is in AP/Bridge mode, it can be configured to authenticate wireless users and distribute encryption keys dynamically by IEEE 802.1x Port-Based Network Access Control and RADIUS (Remote Authentication Dial-In User Service).

- **Repeater.** When the AP is in AP/Bridge mode, it can communicate with other APs or wireless bridges via WDS (Wireless Distribution System). Therefore, an AP can wirelessly forward packets from wireless clients to another AP, and then the later AP forwards the packets to the Ethernet network.

- **Wireless client isolation** When the AP is in AP/Bridge mode, wireless-to-wireless traffic can be blocked so that the wireless clients cannot see each other. This capability can be used in hotspots applications to prevent wireless hackers from attacking other wireless users' computers.

- **AP load balancing** Several APs can form a load-balancing group. Within a group, wireless client associations and traffic load can be shared among the APs. This function is available when the AP is in AP/Bridge mode.

- **Transmit power control.** Transmit power of the AP's RF module can be adjusted to change RF coverage of the AP.

- **Link integrity.** When the AP is in AP/Bridge mode and its Ethernet LAN interface is detected to be disconnected from the wired network, all currently associated wireless clients are disassociated by the AP and no wireless client can associate with it.

- **Association control** When the AP is in AP/Bridge mode, it can be configured to deny

Copyright 2005-2007 ValuePoint Networks, Inc. All rights reserved.

association requests when it has served too many wireless clients or the traffic load is too heavy.

- **Associated wireless clients status.** When the AP is in AP/Bridge mode, it can show the status of all wireless clients that are associated with the AP.
- **N-type (female) external antenna mounts (Not available on IA).** N-type connectors are the industry standard for connection high-gain low-loss antennas indoors or outdoors.
- **Integrated 12dbi or 18dbi high-gain directional antenna (IA only).** AP and directional antenna are sealed in a single rugged and moisture proof case.
- **Antenna alignment assistance (DR only).** The Wireless Network Manager provides a WDS link quality indicator via Wireless Network Manager to facilitate alignment of directional antennas when deploying pairs of wireless bridges.

- **DHCP client.** The AP can automatically obtain an IP address from a DHCP server.
- **DHCP server.** The AP can automatically assign IP addresses to computers or other devices by DHCP (Dynamic Host Configuration Protocol).
  - **Static DHCP mappings.** The administrator can specify static IP address to MAC address mappings so that the specified IP addresses are always assigned to the hosts with the specified MAC addresses.
  - **Current DHCP mappings display.** Shows which IP address is assigned to which host identified by an MAC address.
- **Packet Filtering.** The AP provides Layer 2, Layer 3, and Layer 4 filtering capabilities.
- **Firmware Tools**
  - **Firmware upgrade.** The firmware of the AP can be upgraded via the following methods:
    - **Xmodem-based.** Upgrading firmware over RS232.
    - **TFTP-based.** Upgrading firmware by TFTP (Trivial File Transfer Protocol).
    - **HTTP-based.** Upgrading firmware by HTTP (HyperText Transfer Protocol).
  - **Configuration backup.** The configuration settings of the AP can be backed up to a file via TFTP or HTTP.
  - **Configuration reset.** Resets the AP configuration settings to factory-default values.
- **Management**
  - **Windows-based Wireless Network Manager** for configuring, monitoring, and diagnosing the local computer and neighboring APs. The management protocol is MAC-based.
  - **Web-based Network Manager.** HTTP GUI allows configuring and monitoring the AP via a Web browser. The management protocol is HTTP based.
  - **SNMP.** SNMP (Simple Network Management Protocol) MIB I, MIB II, IEEE 802.1d, IEEE 802.1x, and Private Enterprise MIB are supported.

Copyright 2005-2007 ValuePoint Networks, Inc. All rights reserved.

- **UPnP.** The AP responds to UPnP discovery messages so that a Windows XP user can locate the AP in My Network Places and use a Web browser to configure it.
- **Telnet (Not available on DR).** The user is enabled to manage the AP by Telnet.
- **System log.** For system operational status monitoring.
  - **Local log.** System events are logged to the on-board RAM of the AP and can be viewed using a Web browser.
  - **Remote log by SNMP trap.** Systems events are sent in the form of SNMP traps to a remote SNMP management server.

- **Power over Ethernet.** Supplies power to an AP over an Ethernet cable using IEEE 802.3af compliant technology. This feature facilitates large-scale wireless LAN deployment both indoors and outdoors.
- **Hardware Watchdog Timer.** If the firmware gets stuck in an invalid state, the hardware watchdog timer will detect this situation and restart the AP. This way, the AP can provide continuous services.

LED Definitions

There are several LED indicators inside the housing of the AP. These LEDs are hidden from the public when the AP is deployed to discourage tampering. They are defined as follows, in order from the antenna connector side:

- **PWR**: Power
- **LAN**: Ethernet LAN interface activity
- **RF**: IEEE 802.11 interfaces activity
- **ALV**: *Alive*. Blinks when the AP is working normally.

Copyright 2005-2007 ValuePoint Networks, Inc. All rights reserved.

2. First-Time Installation and Configuration

2.1. Selecting a Power Supply Method

Optionally, you can power the AP with the supplied power adapter or PoE (Power over Ethernet). The AP automatically selects the available one depending on your configuration.

WARNING: The high-power radio in this Access Point requires an attached antenna to function correctly. Running the Access Point with no antenna may damage the radio and reduce maximum radio power.

To power the AP by PoE:

1. Plug one connector of an Ethernet cable to an available port of a PoE hub.
2. Plug the other connector of the Ethernet cable to the **LAN/CONFIG** port of the AP.
3. Tighten the LAN pass-through to prevent moisture from entering the AP

NOTE: The PoE input source to the AP is 48Volt PoE. Applies to all models.

To power the AP by AC power adapter:

1. Remove the solid seal from the AC port in the rugged AP enclosure and replace it with a pass-through seal.
2. Plug the power adapter into an AC socket.
3. Plug the connector of the power adapter to the power jack of the AP.
4. Tighten the AC pass-through to prevent moisture from entering the AP

NOTE: This product is intended to be power-supplied by a Listed Power Unit, marked “Class 2” or “LPS” and output rated “5V DC, 2.5 A ” or equivalent statement.

NOTE: IA models are powered by 48Volt PoE only.

2.2. Mounting the AP on a Wall (Does not apply to IA models)

The AP can be mounted securely on a wall or other solid object indoors or outdoors.

1. Remove the 6 screws attaching AP Top Plate to reveal two mounting holes in opposite corners of the AP.
1. Use mounting screws and anchors of appropriate size for the material the AP is to be mounted on.
2. Replace the Top Plate and secure with the six provided screws.
3. The mounting screws are protected from tampering by the Top Plate, providing additional secu-

Copyright 2005-2007 ValuePoint Networks, Inc. All rights reserved.

rity.

2.3. Connecting Antennas

The SuperAP uses low-loss **Female N-type** antenna connectors. The SuperAP has a single N-type connector, while the DR has two N-type connectors, one for each independent radio. You will need a Male N-type antenna or Male antenna extension cable (pigtail) to attach your antennas to the access point. You can use any type of 2.4GHz rated antenna with the SuperAP from a 1dB "rubber duck" omni to a 36dB satellite dish. Please contact ValuePoint Networks sales for a variety of high-quality antennas that have been tested with the SuperAP.

NOTE (DR only): .The default Access Point radio that subscribers can associate with is WLAN1, which is connected to the Gold (right side) antenna N-type connector.

2.4. Preparing for Configuration

For you to configure an AP, a *managing computer* with a Web browser is needed. For first-time configuration of an AP, an Ethernet network interface card (NIC) should have been installed in the managing computer. For maintenance-configuration of a deployed AP, either a wireless computer or a wired computer can be employed as the managing computer. If the SuperAP Dual Radio (DR) is configured as a Bridge Repeater you must use a wired managing computer.

NOTE: If you are using the browser, *Opera*, to configure an AP, click the menu item **File**, click **Preferences...** click **File types**, and edit the MIME type, **text/html**, to add a file extension ".sht" so that Opera can work properly with the Web management pages of the AP.

Since the configuration/management protocol is HTTP-based, you have to make sure that **the IP address of the managing computer and the IP address of the *managed AP* are in the same IP subnet** (the default IP address of an AP is **192.168.0.1** and the default subnet mask is **255.255.255.0**.) The AP DHCP server is disabled by default, so if you intend to use DHCP, be sure to assign your **managing computer** a static IP address and netmask consistent with the AP. **192.168.0.3** and **255.255.255.0** should work as a static IP to configure that AP is most cases.

2.4.1. Connecting the Managing Computer and the AP

To connect the Ethernet managing computer and the managed AP for first-time configuration, you have two choices as illustrated in Fig. 1.

Copyright 2005-2007 ValuePoint Networks, Inc. All rights reserved.

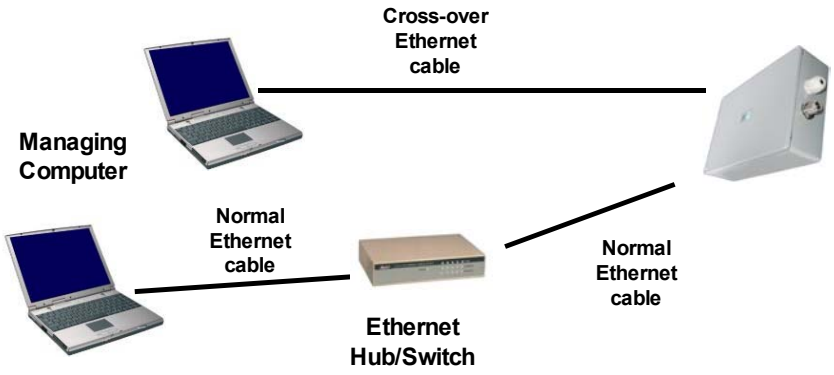


Fig. 1. Connecting a managing computer and an AP via Ethernet.

You can use either a *cross-over* Ethernet cable (we have included one in the package) or a switch/hub with 2 normal Ethernet cables.

NOTE: One connector of the Ethernet cable must be plugged into the **LAN/CONFIG** Ethernet jack of the AP for configuration.

2.4.2. Changing the TCP/IP Settings of the Managing Computer

Use the **Windows Network Control Panel Applet** to change the TCP/IP settings of the managing computer, so that the IP address of the computer and the IP address of the AP are in the same IP sub-net. Set the IP address of the computer to **192.168.0.xxx** (the default IP address of an AP is **192.168.0.1**) and the subnet mask to **255.255.255.0**.

NOTE: For some versions of Windows, the computer needs to be restarted for the changes of TCP/IP settings to take effect.

2.5. Configuring the AP

After the IP addressing issue is resolved, launch a Web browser on the managing computer. Then, go to "**http://192.168.0.1**" to access the *Web-based Network Manager* start page.

Entering the User Name and Password

Before the start page is shown, you will be prompted to enter the user name and password to gain the right to access the Web-based Network Manager. For first-time configuration, use the default user name "**root**" and default password "**root**", respectively.

Copyright 2005-2007 ValuePoint Networks, Inc. All rights reserved.

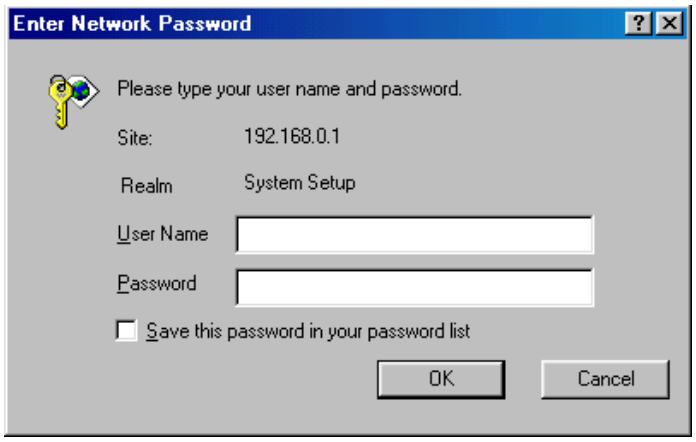


Fig. 2. Entering the user name and password.

NOTE: It is strongly recommended that the password be changed to other value for security reasons. On the start page, click the **General, Password** link to change the value of the password (see Section 3.3.1 for more information).

TIP: Since the start page shows the current settings and status of the AP, it can be saved or printed within the Web browser for future reference.

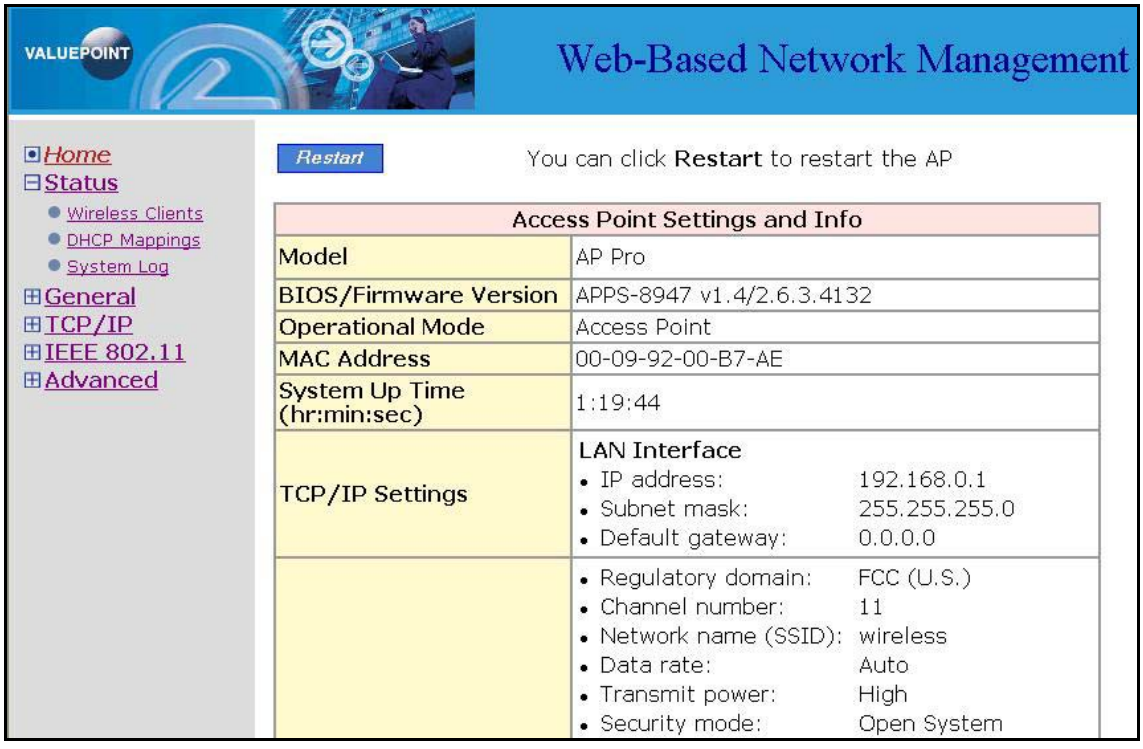


Fig. 3. The Super AP Start page.

2.5.1. Step 1: Selecting an Operational Mode

Go to the **General, Operational Mode** section, select an operational mode and click **Save** at the bottom of this page, and then you are brought back to the start page.

Copyright 2005-2007 ValuePoint Networks, Inc. All rights reserved.

AP Operational Mode (Does not apply to DR model. See next section for DR.)

The SuperAP and IA APs supports 2 operational modes:

- **AP/Bridge.** This mode provides both Access Point and Static LAN-to-LAN Bridging functionality. The static LAN-to-LAN bridging function is supported through Wireless Distribution System (WDS).
- **AP Client.** This mode is for Dynamic LAN-to-LAN Bridging. The AP Client automatically establishes bridge links with APs from any vendors.

Dual Radio Operational Mode (DR Only)

The SuperAP DR supports 3 operational modes:

- **Bridge Repeater.** In this mode, both WLAN interfaces are configured as LAN-to-LAN bridge interfaces. A bridge repeater forwards packets between two wireless LAN-to-LAN bridges. It's possible to use multiple bridge repeaters in between two LAN-to-LAN bridges if the distance is great long.
- **AP Repeater.** In this mode, one WLAN interface is configured as an AP interface, and the other is configured as a LAN-to-LAN bridge interface. The AP repeater is suitable for situations in which Ethernet wiring between the AP and the network backbone is impossible or costs high.
- **Dual AP.** In this mode, both WLAN interfaces are configured as AP interfaces. The dual AP can handle twice the number of wireless clients than a normal AP. It can be treated as "two APs in a box."

The AP forwards packets between its Ethernet interface and wireless interface for wired hosts on the Ethernet side and wireless host(s) on the wireless side.

NOTE: The LAN port MAC Address is the same as WLAN-1. In Dual AP mode the Radios share a single LAN port, so there is just one MAC Address for the LAN interface.

2.5.2. Step 2: Configuring TCP/IP Settings

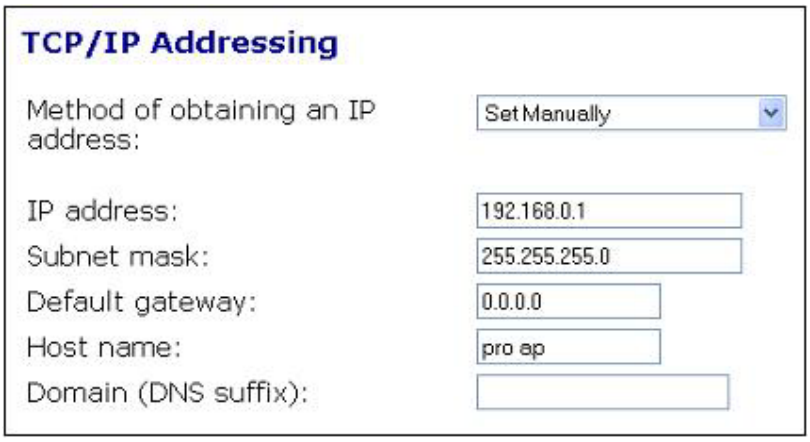


Fig. 4. TCP/IP settings.

Copyright 2005-2007 ValuePoint Networks, Inc. All rights reserved.

Go to the **TCP/IP, Addressing** section to configure IP address settings. The IP address can be manually set or automatically assigned by a DHCP server on the LAN. If you are manually setting the **IP address**, **Subnet mask**, and **Default gateway** settings, set them appropriately, so that they comply with your LAN environment. In addition, you can specify the **Host name** and **Domain (DNS suffix)** of the AP.

When you are finished, click **Save** at the bottom of this page, and then you are brought back to the start page.

2.5.3. Step 3: Configuring IEEE 802.11 Settings

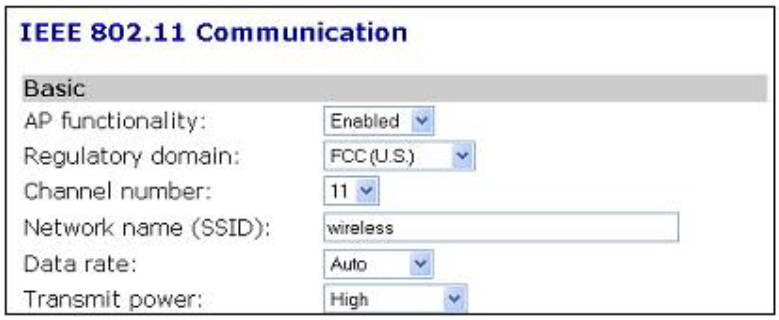


Fig. 5. IEEE 802.11 communication settings.

Go to the **IEEE 802.11, Communication** section to configure IEEE 802.11-related communication settings, including **Regulatory domain**, **Channel number**, and **Network name (SSID)**.

The number of available RF channels depends on local regulations; therefore you have to choose an appropriate regulatory domain to comply with local regulations. **The SSID of a wireless client computer and the SSID of the AP must be identical for them to communicate with each other.**

DR Only: The SuperAP Dual Radio has up to two WLAN interfaces to configure. The following table shows the type of each WLAN interface for each DR operational mode.

	WLAN 1 Interface Type	**WLAN 2 Interface Type**
Bridge Repeater	LAN-to-LAN Bridge	LAN-to-LAN Bridge
AP Repeater	AP	LAN-to-LAN Bridge
Dual AP	AP	AP

DR Only: For a LAN-to-LAN bridge interface, also set the MAC address of each peer bridge according to your planned network topology. Specify an MAC address, and then select its corresponding checkbox. You must have the correct MAC address of its peers entered in each bridge to establish a WDS link.

When you are finished, click **Save** at the bottom of this page, and then you are brought back to the start page.

Copyright 2005-2007 ValuePoint Networks, Inc. All rights reserved.

2.5.4. Step 4: Reviewing and Applying Settings

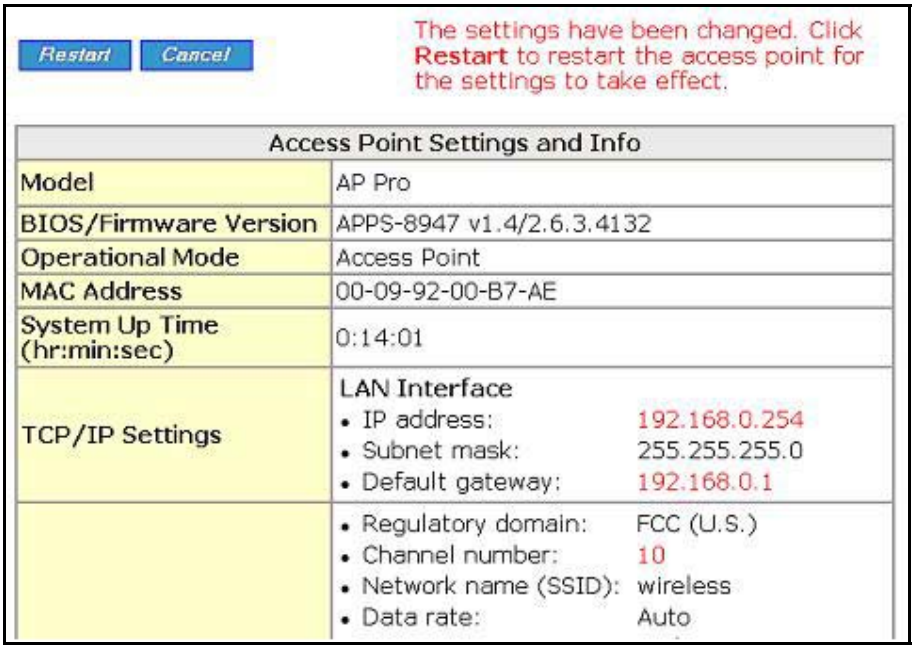


Fig. 6. Settings changes are highlighted in red.

On the start page, you can review all the settings you have made. Changes are highlighted in red. If they are OK, click **Restart** to restart the AP for the new settings to take effect. Click **Cancel** to discard *all* changes.

NOTE: About *7* seconds are needed for the AP to complete its restart process.

2.6. Deploying the AP

After the settings have been configured, deploy the AP to the field application environment. Connect the AP to a LAN segment through an Ethernet switch/hub.

If external high-gain *directional* antennas are used for WDS or LAN-to-LAN bridge interfaces, it may be difficult to adjust the position of the antennas when distance between the AP and its peer is long.

To adjust the position of directional antennas:

1. Connect each device to a computer via Ethernet.
2. Fix the position of the antenna on one side.
3. Adjust the position of the other side by using response time information obtained from PINGing (run PING.exe) the “fixed-side” computer.
4. Fine-tune the position of the antenna until you get the best response time.

Fig. 39 illustrates the idea.

Copyright 2005-2007 ValuePoint Networks, Inc. All rights reserved.

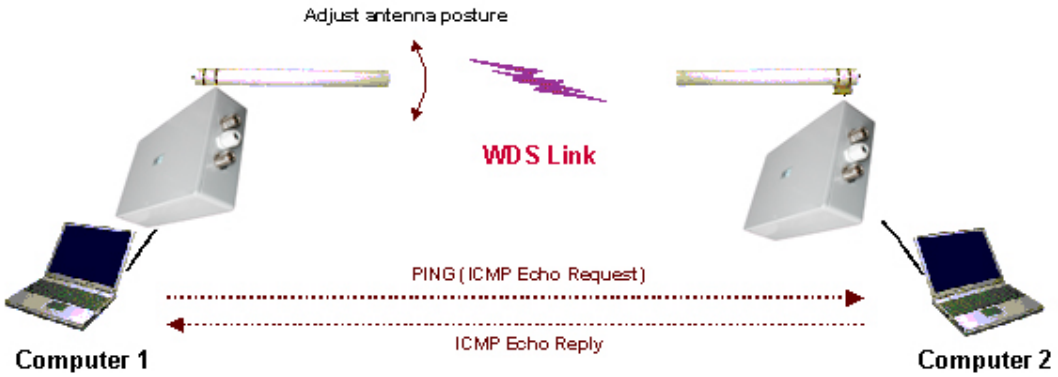


Fig. 7. Adjusting postures of external directional antennas.

NOTE: There are two antenna connectors on one side of the DR, Connector 1, which defaults to SSID wireless1, is the left N-connector. Connector 1 is for the **WLAN 1** interface 1 and Connector 2 is for the **WLAN 2** interface.

2.7. Setting up Client Computers

The TCP/IP and IEEE 802.11-related settings of wireless client computers must match those of the AP.

2.7.1. Configuring IEEE 802.11-Related Settings

Before the TCP/IP networking system of a wireless client computer can communicate with other hosts, the underlying wireless link must be established between this wireless computer and an AP.

To establish a wireless link to an AP:

1. Launch the configuration/monitoring utility provided by the vendor of the installed WLAN NIC.

2. Use the utility to make appropriate *Operating Mode*, *SSID* and *WEP* settings.

NOTE: A wireless client computer must be in *infrastructure* mode, so that it can associate with an AP.

NOTE: The SSID of the wireless client computer and the SSID of the AP must be identical. Or, in case the **SSID broadcasts** capability of the AP is enabled (by default), the SSID of the wireless client computer could be set to "any".

NOTE: Both the wireless client computer and the AP must have the same WEP key settings for them to communicate with each other.

NOTE: For better wireless security, IEEE 802.1x capability of the AP can be enabled so that only authenticated wireless users can access the wireless network. IEEE 802.1x is available on the Adv+ and DR models.

Copyright 2005-2007 ValuePoint Networks, Inc. All rights reserved.

2.7.2. Configuring TCP/IP-Related Settings

Use **Windows Network Control Panel Applet** to change the TCP/IP settings of the client computers, so that the IP addresses of the client computers and the IP address of the AP are in the same IP subnet.

If a client computer is originally set a static IP address, you can either change its IP address to match the IP address of the AP, or select an automatically-obtain-an-IP-address option if there is a DHCP server on the network.

NOTE: For some versions of Windows, the computer needs to be restarted for the changes to TCP/IP settings to take effect.

2.8. Confirming the Settings of the AP and Client Computers

After you have completed deploying the AP and setting up client computers, you have to make sure the settings you have made are correct.

2.8.1. Checking if the IEEE 802.11-Related Settings Work

To check if a wireless client computer can associate with the AP:

1. Launch the configuration/monitoring utility provided by the vendor of the installed WLAN NIC.

2. Check if the client computer is associated to an access point, and the access point is the AP.

If the check fails, see Appendix B-1, “Wireless Settings Problems” for troubleshooting.

2.8.2. Checking if the TCP/IP-Related Settings Work

To check if a client computer can access the Internet:

1. Open a **Windows Command Prompt** window on the client computer.

2. Type “**ping** *advap*”, where *advap* is a placeholder for the IP address of the AP. Replace it with your real IP address—for example, 192.168.0.1. Then press **Enter**.

   If the AP responds, go to the next step; else, see Appendix B-2, “TCP/IP Settings Problems” for troubleshooting.

3. Type “**ping** *default_gateway*”, where *default_gateway* is a placeholder for the IP address of the default gateway of the wireless client computer. Then press **Enter**.

   If the gateway responds, go to the next step; else, see Appendix B-2, “TCP/IP Settings Problems” for troubleshooting.

4. Type “**ping** *1st_dns_server*”, where *1st_dns_server* is a placeholder for the IP address of the primary DNS server of the wireless client computer. Then press **Enter**.

   If this DNS server responds the client should have no problem with TCP/IP networking; else, see Appendix B-2, “TCP/IP Settings Problems” for troubleshooting.

Copyright 2005-2007 ValuePoint Networks, Inc. All rights reserved.

2.9. Resetting the Access Point to Factory Default

If the Access Point becomes unresponsive in use or after making changes to the configuration you can reboot the access point by hardware or software. If resetting does not resolve the problem, or the AP becomes unreachable, can reset the AP to its factory defaults.

Soft Reset

You can reboot or restore factory defaults by selecting these options in the management interface.

Hard Reset

Hard Reboot

Remove the watertight reset button seal from the outside of the enclosure and press the reset button. It takes a few seconds for the AP to reboot.

Hard Reset to Factory Defaults

When the AP is on you can reset the AP to the factory settings by holding the reset button for approximately ten seconds. When you release the button the AP will be reset to the factory defaults, so change you managing computer's IP settings accordingly to access the AP management interface.

Copyright 2005-2007 ValuePoint Networks, Inc. All rights reserved.

3. Using The Web-Based Network Manager

In this chapter, we'll explain each Web management page of the Web-based Network Manager.

Overview

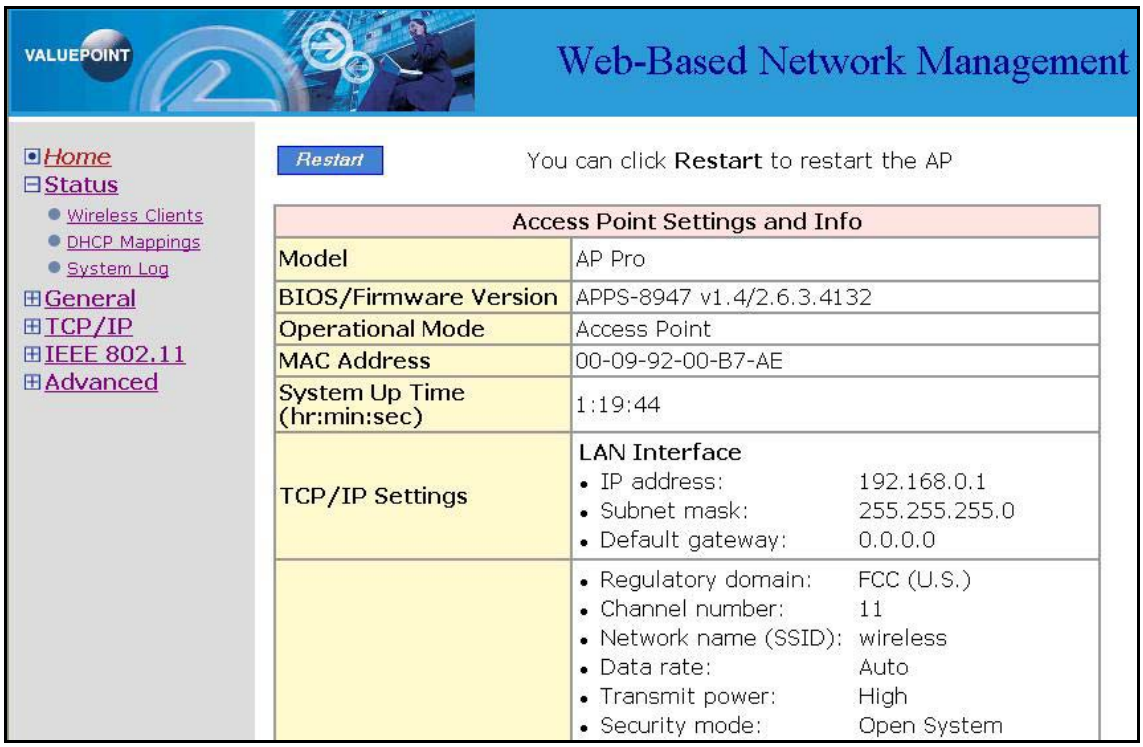


Fig. 8. The SuperAP Start page.

Menu Structure

The left side of the start page contains a menu for you to carry out commands. Here is a brief description of the hyperlinks on the menu:

- **Home.** For going back to the start page.
- **Status.** Status information.
  - **Wireless Clients.** The status of the wireless clients currently associated with the AP.
  - **DHCP Mappings.** Current IP-MAC address mappings of the built-in DHCP server.
  - **System Log.** System events log.
  - **Link Monitor.** Signal strength and quality of Client Mode connection.
- **General.** Global operations.
  - **Operation Mode.** For setting the AP to Client, Bridge, or AP modes.

Copyright 2005-2007 ValuePoint Networks, Inc. All rights reserved.

- **Password.** For gaining rights to change the settings of the AP.
- **Firmware Tools.** For upgrading the firmware of the AP, backing up and restoring configuration, and configuration reset settings of the AP.

- **TCP/IP.** TCP/IP-related settings.
  - **Addressing.** IP address settings for the AP to work with TCP/IP.
  - **DHCP Server.** Settings for the DHCP (Dynamic Host Configuration Protocol) server on the AP.

- **IEEE 802.11.** IEEE 802.11-related settings.
  - **Communication.** Basic settings for the IEEE 802.11 interface of the AP to work properly with wireless clients.
  - **Security.** Security settings for authenticating wireless users and encrypting wireless data.
  - **IEEE 802.1x/RADIUS** IEEE 802.1x Port-Based Network Access Control and RADIUS (Remote Authentication Dial-In User Service) settings for better wireless security.

- **Advanced.** Advanced settings of the AP.
  - **Packet Filters.** Ethernet Type Filters, IP Protocol Filters, and TCP/UDP Port Filters settings.
  - **Management.** UPnP, System Log, and SNMP settings.

3.1.1.1. Save, Save & Restart, and Cancel Commands

Fig. 9. Save, Save & Restart, and Cancel.

At the bottom of each page that contains settings you can configure, there are up to three buttons—**Save**, **Save & Restart**, and **Cancel**. Clicking **Save** stores the settings changes to the memory of the AP and brings you back to the start page, where you can review any changes in red. Clicking **Save & Restart** stores the settings changes to the memory of the AP and restarts the AP immediately. Clicking **Cancel** discards any settings changes and brings you back to the start page.

If you click **Save**, the start page will reflect the fact that the configuration settings have been changed by showing two buttons—**Restart** and **Cancel**. In addition, changes are highlighted in red. Clicking **Cancel** discards all the changes. Clicking **Restart** restarts the AP for the settings changes to take effect.

Copyright 2005-2007 ValuePoint Networks, Inc. All rights reserved.

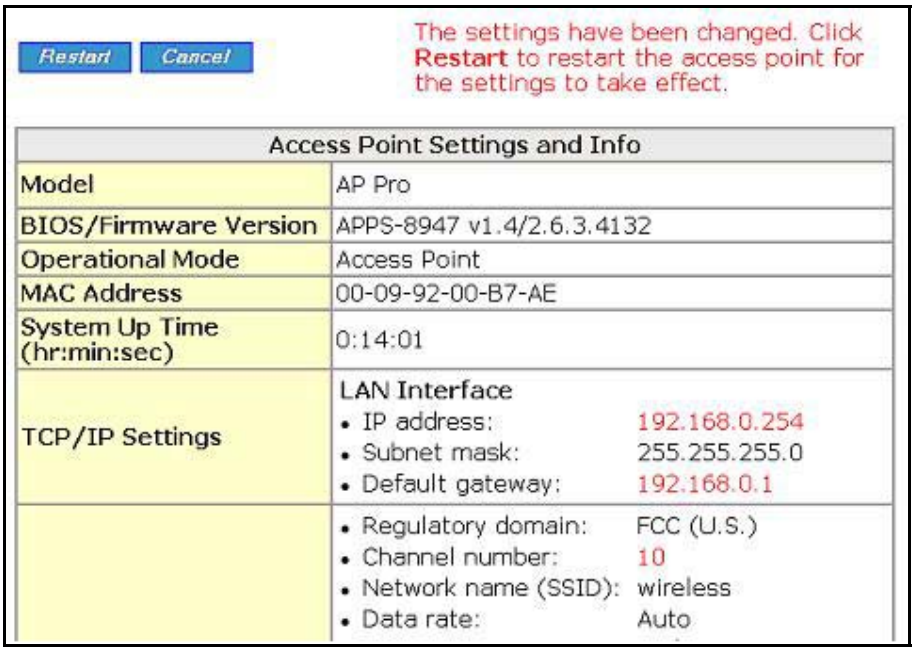


Fig. 10. Settings have been changed.

3.1.1.2. Home and Refresh Commands

Fig. 11. Home and Refresh.

At the bottom of each status page that shows read-only information, there are two buttons—**Home** and **Refresh**. Clicking **Home** brings you back to the start page. Clicking **Refresh** updates the shown status information.

3.2. AP Status

3.2.1. Associated Wireless Clients

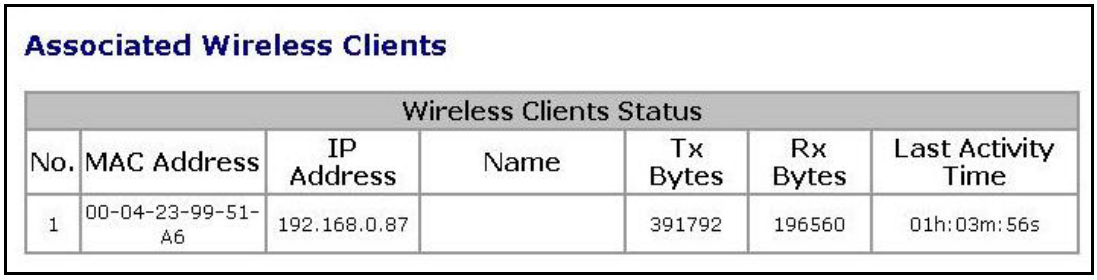


Fig. 12. Status of associated wireless clients.

On this page, the status information of each associated client, including its MAC address, IP address, user name (if the client has been IEEE 802.1x authenticated), number of bytes it has send, number of

Copyright 2005-2007 ValuePoint Networks, Inc. All rights reserved.

bytes it has received, and the time of its last activity, is shown.

3.2.2. Current DHCP Mappings

DHCP Mapping Table			
No.	MAC Address	IP Address	Type
1	00-90-4B-00-B9-BD	192.168.168.214	Static
2	00-BB-DE-AD-BE-EF	192.168.168.224	In use
3	00-90-4B-00-40-94	192.168.168.226	Dynamic
4	00-40-01-43-1D-E8	192.168.168.230	In use

Fig. 13. Current DHCP mappings.

On this page, all the current *static* or *dynamic* DHCP mappings are shown. A DHCP mapping is a correspondence relationship between an IP address assigned by the DHCP server and a computer or device that obtains the IP address. A computer or device that acts as a DHCP client is identified by its MAC address.

A static mapping indicates that the DHCP client always obtains the specified IP address from the DHCP server. You can set static DHCP mappings in the **Static DHCP Mappings** section of the **DHCP Server** configuration page (see Section 3.4.2). A dynamic mapping indicates that the DHCP server chooses an IP address from the IP address pool specified by the **First allocateable IP address** and **Allocateable IP address count** settings on the **DHCP Server** configuration page.

3.2.3. System Log

System Log

Model:	AP Pro
BIOS/Firmware version:	APPS-8947 v1.4/2.6.3.4132
Operational mode:	Access Point
Current time:	Wednesday, March 24, 2004 5:02:06 PM

Wednesday, March 24, 2004 3:09:10 PM SYSTEM START UP!
Wednesday, March 24, 2004 3:09:10 PM Wireless LAN interface initializes success.
Wednesday, March 24, 2004 3:09:10 PM Mac address --> 00-09-92-00-B7-AE
Wednesday, March 24, 2004 3:09:10 PM LAN IP address --> 192.168.0.1.
Wednesday, March 24, 2004 3:09:30 PM Wireless client 00-04-23-99-51-A6 is associated with.
Wednesday, March 24, 2004 3:10:32 PM Wireless client 00-04-23-99-51-A6 is disassociated with.
Wednesday, March 24, 2004 3:10:42 PM Wireless client 00-04-23-99-51-A6 is associated with.
Wednesday, March 24, 2004 3:10:51 PM The administrator from 192.168.0.87 logins the device successfully.

Fig. 14. System log.

System events are recorded in the memory of the AP. The logged information is useful for trouble-shooting purposes. The system events are divided into several categories, and you can select which categories of events to log. See Section 3.6.2.2 for more information.

Copyright 2005-2007 ValuePoint Networks, Inc. All rights reserved.

3.2.4. Link Monitor

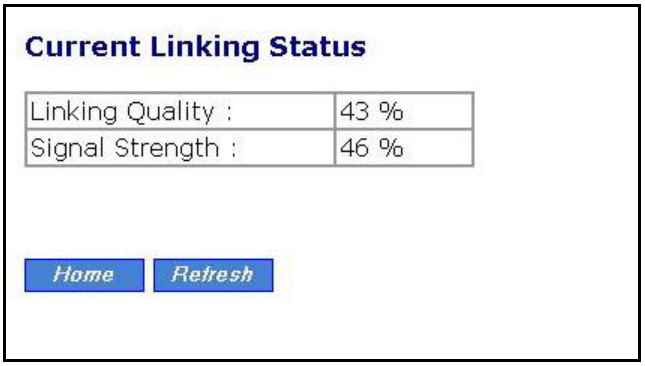


Fig. 15. SuperAP Operational modes settings.

When the SuperAP is in Client Mode, this page displays the current signal strength and quality of the link to the host access point.

3.3. General Operations

3.3.1. Specifying Operational Mode

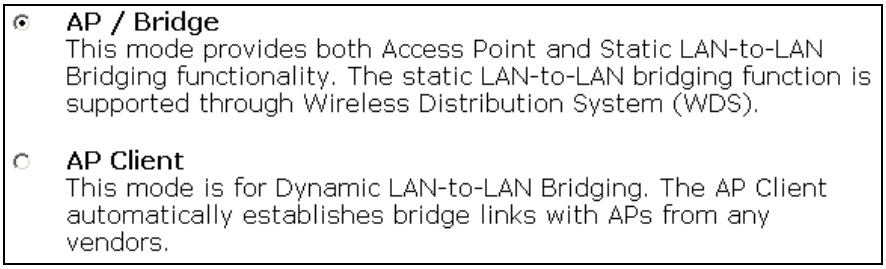

AP / Bridge
This mode provides both Access Point and Static LAN-to-LAN Bridging functionality. The static LAN-to-LAN bridging function is supported through Wireless Distribution System (WDS).
AP Client
This mode is for Dynamic LAN-to-LAN Bridging. The AP Client automatically establishes bridge links with APs from any vendors.

Fig. 16. SuperAP Operational modes settings.

AP Operational Mode (Does not apply to DR model. See below for DR.)

The AP supports 2 operational modes:

- **AP/Bridge.** This mode provides both Access Point and Static LAN-to-LAN Bridging functionality. The static LAN-to-LAN bridging function is supported through Wireless Distribution System (WDS).
- **AP Client.** This mode is for Dynamic LAN-to-LAN Bridging. The AP Client automatically establishes bridge links with APs from any vendors.

Copyright 2005-2007 ValuePoint Networks, Inc. All rights reserved.

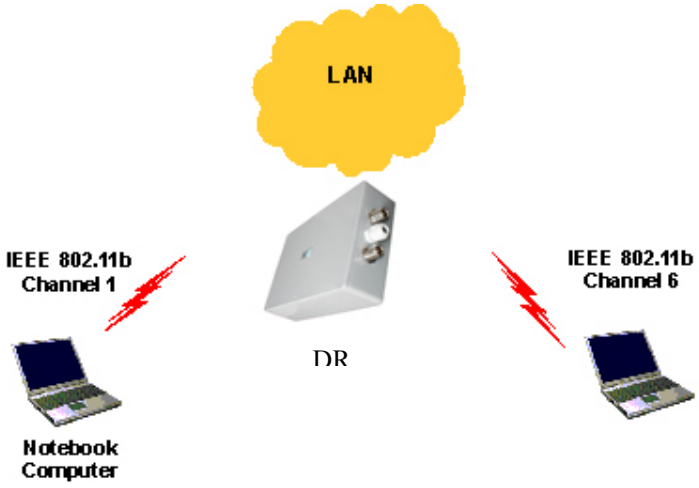
Dual Radio Operational Mode (DR Only)

The DR supports 3 operational modes:

- **Bridge Repeater.** In this mode, both WLAN interfaces are configured as LAN-to-LAN bridge interfaces. A bridge repeater forwards packets between two wireless LAN-to-LAN bridges. It's possible to use multiple bridge repeaters in between two LAN-to-LAN bridges if the distance is great long.

- **AP Repeater.** In this mode, one WLAN interface is configured as an AP interface, and the other is configured as a LAN-to-LAN bridge interface. The AP repeater is suitable for situations in which Ethernet wiring between the AP and the network backbone is impossible or costs high.

- **Dual AP.** In this mode, both WLAN interfaces are configured as AP interfaces. The dual AP can handle twice the number of wireless clients than a normal AP. It can be treated as "two APs in a box."



Copyright 2005-2007 ValuePoint Networks, Inc. All rights reserved.

The AP forwards packets between its Ethernet interface and wireless interface for wired hosts on the Ethernet side and wireless host(s) on the wireless side.

There are 2 types of wireless links as specified by the IEEE 802.11 standard.

- **STA-AP.** This type of wireless link is established between an IEEE 802.11 Station (STA) and an IEEE 802.11 Access Point (AP). An STA is usually a client computer (PC or PDA) with a WLAN network interface card (NIC). The AP in Client mode is actually an STA, allowing greater compatibility with other brands of APs.

- **WDS.** This type of wireless link is established between two IEEE 802.11 APs. Wireless packets transmitted along the WDS link comply with the IEEE 802.11 WDS (Wireless Distribution System) format at the link layer.

The relationships among the operational modes and the wireless link types are shown in the following table:

	AP/Bridge	AP Client
AP/Bridge, AP Repeater	WDS	STA-AP
AP Client	STA-AP	
Bridge Repeater	WDS	
Dual AP		STA-AP

Table 1. Operational modes vs. wireless link types.

To establish a *static* bridge link based on WDS, the AP/bridges at both end of the WDS link must be *manually* configured with each other's MAC addresses (see Section 3.5.1.6 for more information). To establish a *dynamic* bridge link between an AP and an AP Client, both devices have to be configured with the same SSID and WEP settings. The AP Client automatically scans for any AP that is using the matched SSID and establishes a bridge link with the scanned AP.

NOTE: Although it's more convenient to use dynamic bridging, it has a limitation—the AP Client only can forward TCP/IP packets between its wireless interface and Ethernet interface; other types of traffic (such as IPX and AppleTalk) are not forwarded.

TIP: When the AP is configured to be in AP Client, it can be used as an Ethernet-to-wireless network adapter. For example, a notebook computer equipped with an Ethernet adapter can be connected to this device with a crossover Ethernet cable for wireless connectivity to another access point.

Copyright 2005-2007 ValuePoint Networks, Inc. All rights reserved.

3.3.2. Changing Password

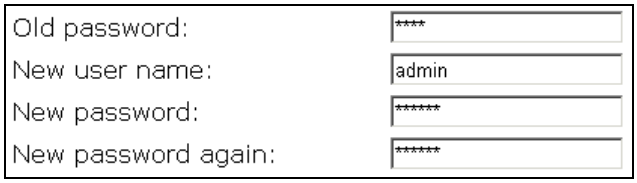


Fig. 17. Password.

On this page, you can change the user name and password for the right to modify the configuration of the bridge. The new password must be typed twice for confirmation.

3.3.3. Managing Firmware

Fig. 18. Firmware management protocol setting.

Firmware management operations for the AP include *firmware upgrade*, *configuration backup*, *configuration restore*, and *configuration reset*. Firmware upgrade, configuration backup, and configuration restore can be achieved via HTTP or TFTP. The HTTP-based way is suggested because it is more user friendly. However, due to different behavior of different Web browser types and versions, HTTP-based firmware management operations may not work properly with some Web browsers. If you cannot successfully perform HTTP-based firmware management operations with your Web browser, try the TFTP-based way.

3.3.3.1. Upgrading Firmware via HTTP

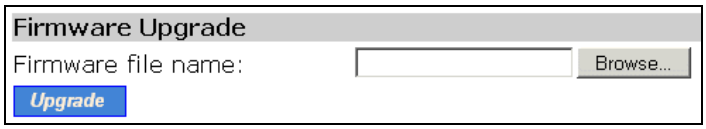


Fig. 19. Firmware upgrade via HTTP.

To upgrade firmware of the AP via HTTP:

1. Click **Browse** and then select a correct firmware **.bin** file. The firmware file path will be shown in the **Firmware file name** text box.

2. Click **Upgrade** to begin the upgrade process.

3.3.3.2. Backing up and Restoring Configuration Settings via HTTP

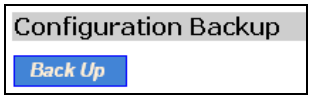


Fig. 20. Firmware backup via HTTP.

Copyright 2005-2007 ValuePoint Networks, Inc. All rights reserved.

To back up configuration of the AP via HTTP:

1. Click **Back Up**.

2. You'll be prompted to open or save the configuration file. Click **Save**.

3. The configuration file is named by the AP's MAC address. For example, if the AP's MAC address is 00-01-02-33-44-55, the configuration backup file should be "000102334455.hex". Don't change the configuration file name in the **Save As** dialog box. Select a folder in which the configuration file is to be stored. Then, click **Save**.

NOTE: The procedure may be a little different with different Web browsers.

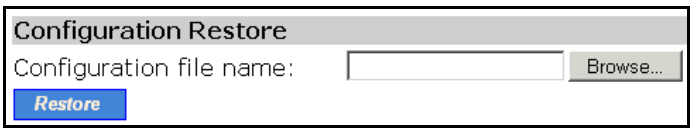


Fig. 21. Configuration restore via HTTP.

To restore configuration of the AP via HTTP:

1. Click **Browse** and then select a correct configuration **.hex** file. You have to make sure the file name is the AP's MAC address. The firmware file path will be shown in the **Firmware file name** text box.

2. Click **Restore** to upload the configuration file to the AP.

3.3.3.3. Upgrading Firmware via TFTP

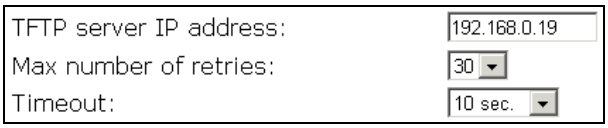


Fig. 22. TFTP server settings.

When use TFTP as the firmware management protocol, you can configure settings for the AP's TFTP client to communicate with a TFTP server. If the TFTP client does not get a response from the TFTP server within a period specified by the **Timeout** setting, it will resend the previous request. The **Max number of retries** setting specifies the maximal number of resend before the TFTP client stops communicating with the TFTP server.

Please note that you will need to run a TFTP Server at the specified address.

Fig. 23. Firmware upgrade via TFTP.

To upgrade firmware of the AP via TFTP:

1. Set up a computer that will be used as a TFTP server and as a managing computer to trigger the upgrade process.

Copyright 2005-2007 ValuePoint Networks, Inc. All rights reserved.

2. Connect the computer and one of the LAN Ethernet switch port with an Ethernet cable.

3. Configure IP address of the computer so that the AP and the computer are in the same IP subnet.

4. On the computer, run the TFTP Server utility. And specify the folder in which the firmware files reside.

5. On the computer, run a Web browser, log on to the AP, and click the **General, Firmware Tools** hyperlink.

6. Choose **TFTP** as the **Firmware management protocol**.

7. Specify the IP address of the computer, which acts as a TFTP server. If you don't know the IP address of the computer, open a Command Prompt, and type IpConfig, then press the **Enter** key.

8. Trigger the firmware upgrade process by clicking **Upgrade**.

NOTE: The LAN IP address of the AP and the IP address of the TFTP server must be in the same IP subnet for TFTP to work.

NOTE: Due to the unreliable nature of wireless media, it's highly recommended that the TFTP server and the to-be-upgraded wireless AP be connected by Ethernet, and on the same LAN.

NOTE: After the firmware is upgraded, be sure to delete the contents of the Web browser cache, so that the Web management pages can be shown correctly.

NOTE: A failed upgrade may corrupt the firmware and make the AP unusable. If this occurs, please contact technical support.

3.3.3.4. Backing up and Restoring Configuration Settings by TFTP

Fig. 24. Configuration backup/restore.

To back up configuration of the AP by TFTP:

1. Set up a computer that will be used as a TFTP server and as a managing computer to trigger the upgrade process.

2. Connect the computer and one of the LAN Ethernet switch port with an Ethernet cable.

3. Configure IP address of the computer so that the AP and the computer are in the same IP subnet.

4. On the computer, run the TFTP Server utility. And specify the folder in which the firmware files reside.

5. On the computer, run a Web browser, log on to the AP, and click the **General, Firmware Tools** hyperlink.

Copyright 2005-2007 ValuePoint Networks, Inc. All rights reserved.

6. Choose **TFTP** as the **Firmware management protocol**.

7. Within the **Configuration Backup/Restore** section, specify the IP address of the computer, which acts as a TFTP server. If you don't know the IP address of the computer, open a Command Prompt, and type IpConfig, then press the **Enter** key.

8. Trigger the backup process by clicking **Back Up**. The AP's configuration settings will be saved as "**AaBbCcDdEeFf.hex**" by the TFTP server, where "AaBbCcDdEeFf" is the AP's MAC address. For example, if the AP's MAC address is 00-01-02-33-44-55, the configuration backup file will be "000102334455.hex".

To restore configuration of the AP by TFTP:

1. Set up a computer that will be used as a TFTP server and as a managing computer to trigger the upgrade process.

2. Connect the computer and one of the LAN Ethernet switch port with an Ethernet cable.

3. Configure IP address of the computer so that the AP and the computer are in the same IP subnet.

4. On the computer, run the TFTP Server utility and specify the folder in which the configuration backup file resides. A configuration backup file is named by the AP's MAC address. For example, if the AP's MAC address is 00-01-02-33-44-55, the configuration backup file should be "000102334455.hex".

5. On the computer, run a Web browser, log on to the AP, and click the **General, Firmware Tools** hyperlink.

6. Choose **TFTP** as the **Firmware management protocol**.

7. Within the **Configuration Backup/Restore** section, specify the IP address of the computer, which acts as a TFTP server. If you don't know the IP address of the computer, open a Command Prompt, and type IpConfig, then press the **Enter** key.

8. Trigger the restoring process by clicking **Restore**. The AP will then download the configuration backup file from the TFTP server.

NOTE: Make sure the file is a valid configuration backup file for the AP.

3.3.3.5. Resetting Configuration to Factory Defaults

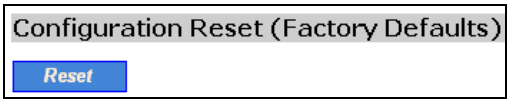


Fig. 25. Configuration reset.

Clicking the **Reset** button resets the device configuration to factory defaults.

WARNING: When you click the **Reset** you will lose all your current configuration settings.

Copyright 2005-2007 ValuePoint Networks, Inc. All rights reserved.

3.4. Configuring TCP/IP Related Settings

3.4.1. Addressing

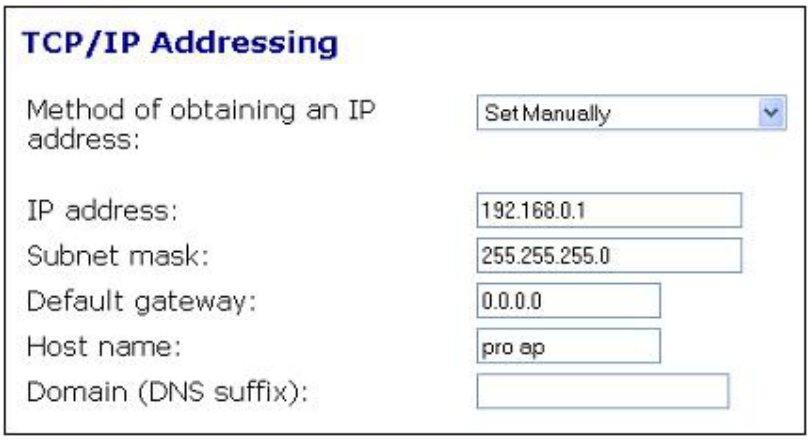


Fig. 26. TCP/IP settings.

The IP address of the AP can be manually set (**Set Manually**) or automatically assigned by a DHCP server on the LAN (**Obtain from a DHCP Server**). If you are manually setting the **IP address**, **Subnet mask**, and **Default gateway** settings, set them appropriately, so that they comply with your LAN environment. In addition, you can specify the **Host name** and **Domain (DNS suffix)** of the AP.

3.4.2. DHCP Server

3.4.2.1. Basic

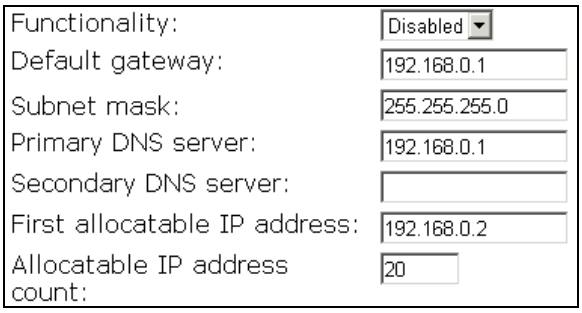


Fig. 27. Basic DHCP server settings.

The AP can automatically assign IP addresses to client computers by DHCP. In this section of the management page, you can specify the **Default gateway**, **Subnet mask**, **Primary DNS server**, and **Secondary DNS server** settings that will be sent to a client at its request. Additionally, you can specify the first IP address that will be assigned to the clients and the number of allocateable IP addresses.

NOTE: There should be only *one* DHCP server on the LAN; otherwise, DHCP will not work properly. If there is already a DHCP server on the LAN, disable the DHCP server functionality of the AP.

NOTE: By default the DHCP server function is disabled.

Copyright 2005-2007 ValuePoint Networks, Inc. All rights reserved.

3.4.2.2. Static DHCP Mappings

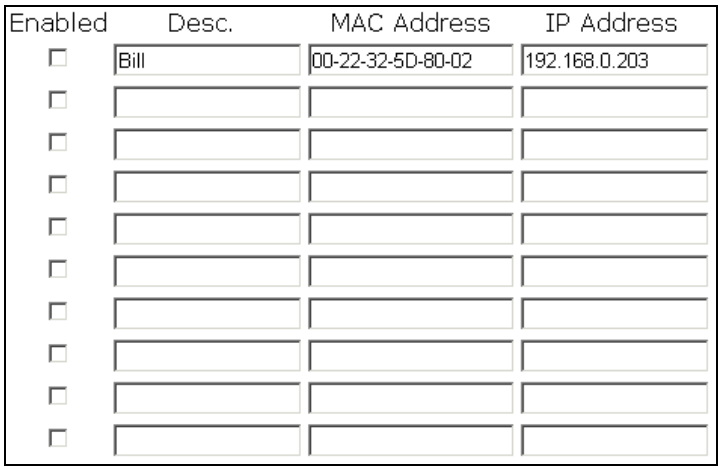


Fig. 28. Static DHCP mappings.

IP addresses of servers are often static so that clients could always locate the servers by the static IP addresses. Using **Static DHCP Mappings**, you can ensure that a host will get the same IP address when it requests one from the DHCP server. Therefore, instead of configuring the IP address of a server manually, you can configure the server to obtain an IP address by DHCP and it is always assigned the same IP address.

To always assign a static IP address to a specific DHCP client:

1. Specify the MAC address of the DHCP client and the IP address to be assigned to it. You can provide a text description for this mapping, if desired.

2. Select the corresponding **Enabled** check box.

NOTE: You will need to enable the new Static IP entries to save them. New entries will overwrite old entries not currently enabled.

3.5. Configuring IEEE 802.11-Related Settings

3.5.1. Communication

3.5.1.1. Basic

Basic IEEE 802.11-related communication settings include **AP functionality**, **Regulatory domain**, **Channel number**, **Network name (SSID)**, **Data rate**, and **Transmit power**.

Copyright 2005-2007 ValuePoint Networks, Inc. All rights reserved.

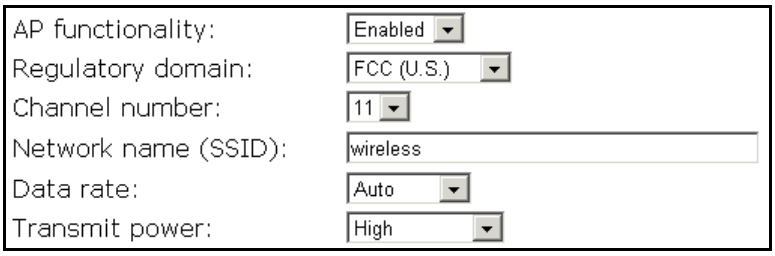


Fig. 29. Basic IEEE 802.11 communication settings.

For specific needs such as configuring the AP as a wireless LAN-to-LAN bridge, the AP functionality can be disabled, so that no wireless client can associate with the AP.

The number of available RF channels depends on local regulations; therefore you have to choose an appropriate regulatory domain to comply with local regulations. The SSID of a wireless client computer and the SSID of the AP must be identical for them to communicate with each other.

The transmit power of the RF module in the AP can be adjusted so that the RF coverage of the AP can be changed.

Transmit Power	Output (dBm)
High	22-23
Medium High	17-18
Medium	14-15
Medium Low	11-12
Low	8-9

If desired, you can manually set the data rate supported by the AP.

3.5.1.2. Client Mode Settings

When the AP is in Wireless Client mode there are a limited number of settings, similar to what you would find on your Laptop Wireless Client. You can select Site Survey to see available SSIDs that the Client Mode AP can associate with.

3.5.1.3. Link Integrity

Fig. 30. Link integrity settings.

When the Ethernet LAN interface is disconnected from the wired network, the AP disassociates all currently associated wireless clients and no wireless client can associate with the AP. The detection mechanism is based on pinging the IP address specified in **Reference host**.

Copyright 2005-2007 ValuePoint Networks, Inc. All rights reserved.

3.5.1.4. Association Control

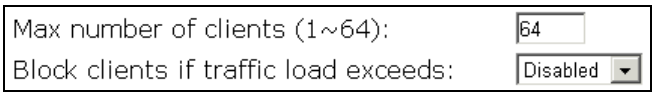


Fig. 31. Association control settings.

If the number of currently associated wireless clients equals the value specified in the **Max number of clients** setting, no more wireless client can associate with the AP. If traffic load of the AP exceeds the load specified in the **Block clients if traffic load exceeds** setting, no more wireless clients can associate with the AP until traffic is reduced.

3.5.1.5. AP Load Balancing

Fig. 32. AP load balancing settings.

Several APs can form a load-balancing group if they are set with the same **Group ID**. The load-balancing policy can be by **Number of Users** or by **Traffic Load**.

If the *by-number-of-users* policy is selected, a new wireless user can only associate with an AP that has the smallest number of associated wireless users in the group. On the other hand, if the *by-traffic-load policy* is selected, a new wireless user can only associate with an AP that has the lowest traffic load in the group.

3.5.1.6. Wireless Distribution System

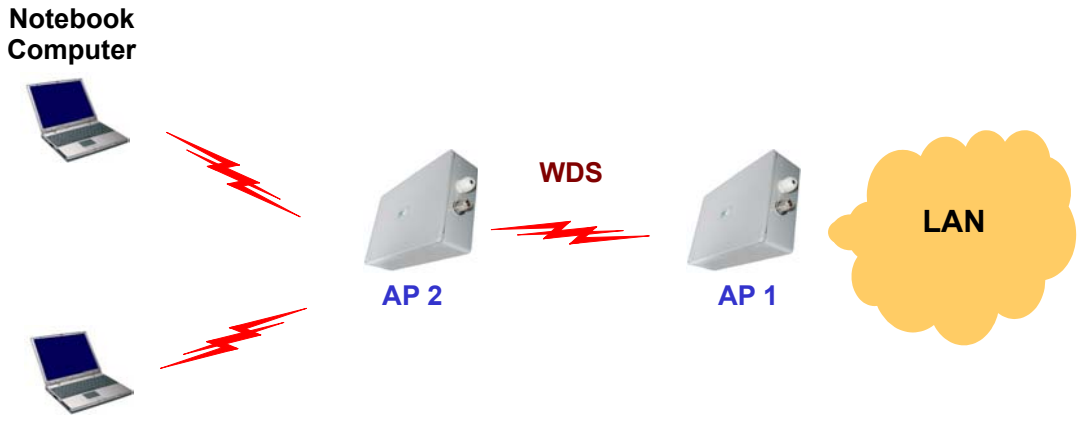


Fig. 33. Wireless Distribution System.

Traditionally, access points are connected by Ethernet. By Wireless Distribution System (WDS), APs can communicate with one another wirelessly. For example, in Fig. 33, AP 2 acts as an access point for the notebook computers and it forwards packets sent from the notebook computers to AP 1 through WDS. Then, AP 1 forwards the packets to the Ethernet LAN. Packets destined for the notebook computers follow a reverse path from the Ethernet LAN through the APs to the notebook com-

Copyright 2005-2007 ValuePoint Networks, Inc. All rights reserved.

puters. In this way, AP 2 plays a role of "AP repeater".

Fig. 34. LAN-to-LAN bridging.

By WDS, two or more LAN segments can be connected wirelessly. As illustrated in Fig. 34, a pair of wireless LAN-to-LAN bridges is used to connect two LAN segments. Since the AP is WDS-enabled it can be used as a wireless bridge.

NOTE: An AP can have up to *6* WDS links to other APs or wireless bridges.

TIP: Just because you *can* have 6 WDS links does not means you *should* have 6 WDS links. One AP Radio only has 11Mbps of total bandwidth, and it must be divided between WDS and any connected clients on that AP. Using the DR for WDS ameliorates this problem by providing a dedicated WDS Link.

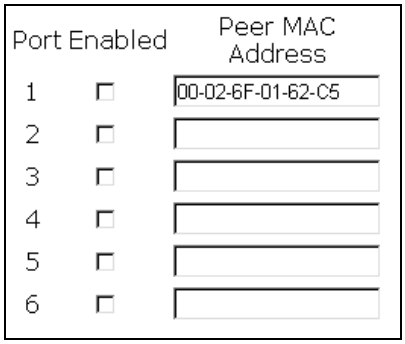


Fig. 35. Wireless Distribution System settings.

To enable a WDS link:

1. Specify the MAC address of the AP at the other end of the WDS link.

2. Select the corresponding **Enabled** check box.

3. Repeat for AP on the other end.

For example, assume you want two APs with MAC addresses 00-02-65-01-62-C5 and 00-02-65-01-62-C6 to establish a WDS link between them. On AP 00-02-65-01-62-C5, set the peer MAC address of port 1 to 00-02-65-01-62-C6 and on AP 00-02-65-01-62-C6, set the peer MAC address of port 1 to 00-02-65-01-C5.

Copyright 2005-2007 ValuePoint Networks, Inc. All rights reserved.

TIP: Plan your wireless network and draw a diagram, so that you know how a bridge is connected to other peer bridges by WDS. See the following figure for an example network-planning diagram.

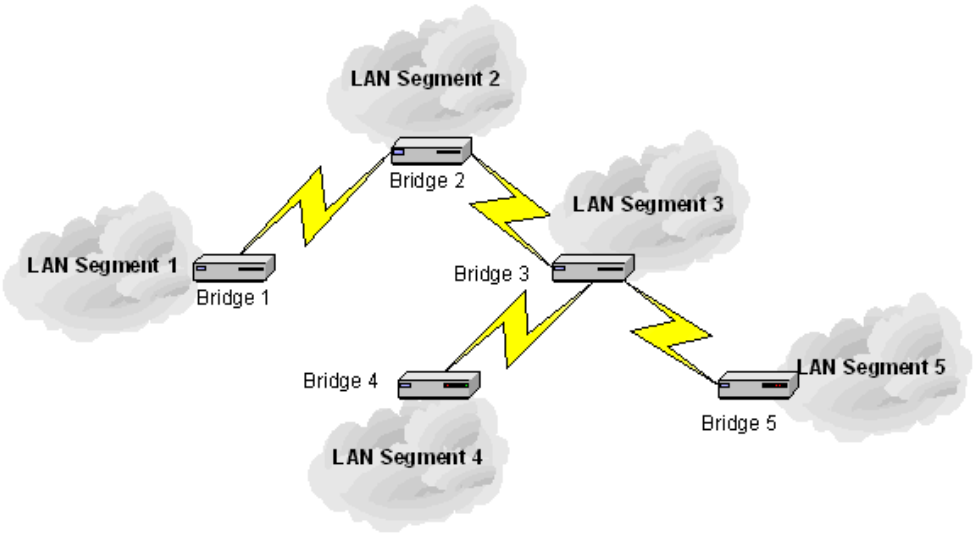


Fig. 36. Sample wireless bridge network topology.

WARNING: Don't let your network topology consisting of wireless bridges, Ethernet switches, Ethernet links, and WDS links contain *loops*. If any loops exist, packets will circle around the loops and network performance will be seriously degraded.

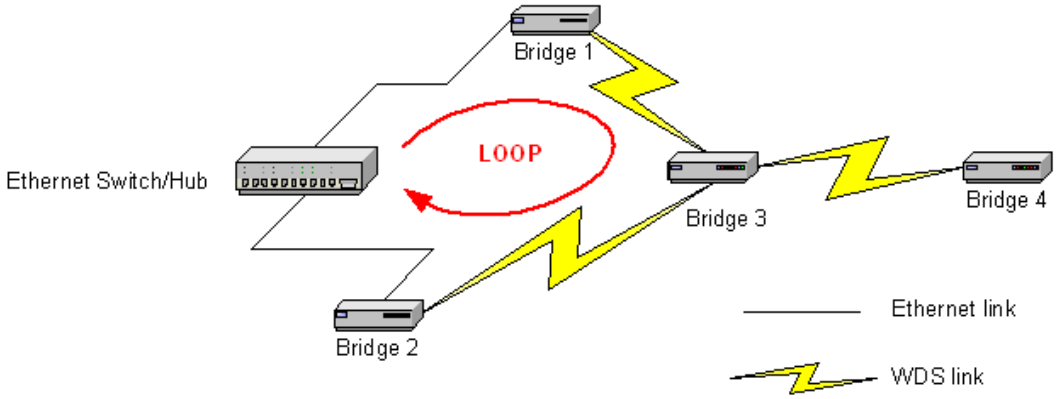


Fig. 37. Network topology containing a loop.

If external high-gain *directional* antennas are used, it can be difficult to align the antennas when the distance between the bridges is long.

3.5.1.7. Antenna Alignment

There are many methods that can be used to align outdoor antenna to achieve the best possible signal. We have outlined two below. Using the built-in Antenna Alignment feature in the SuperAP Wireless Network Manager is the most convenient, but requires access to a Windows host PC.

Copyright 2005-2007 ValuePoint Networks, Inc. All rights reserved.

Aligning External Antennas using WNM

When deploying the DR, instead of using PING.exe you can run the Wireless Network Manager on Computer 1, and go to the **Antenna Alignment** tab. Click **Start** to begin monitoring the WDS link quality. Adjust the posture of the antenna of Bridge 1 until the **Link quality** indicator shows a *relatively* maximal value. Finally, click **Stop** to stop monitoring WDS link quality. You can repeat this for Bridge 2 in Bridge Repeater mode.

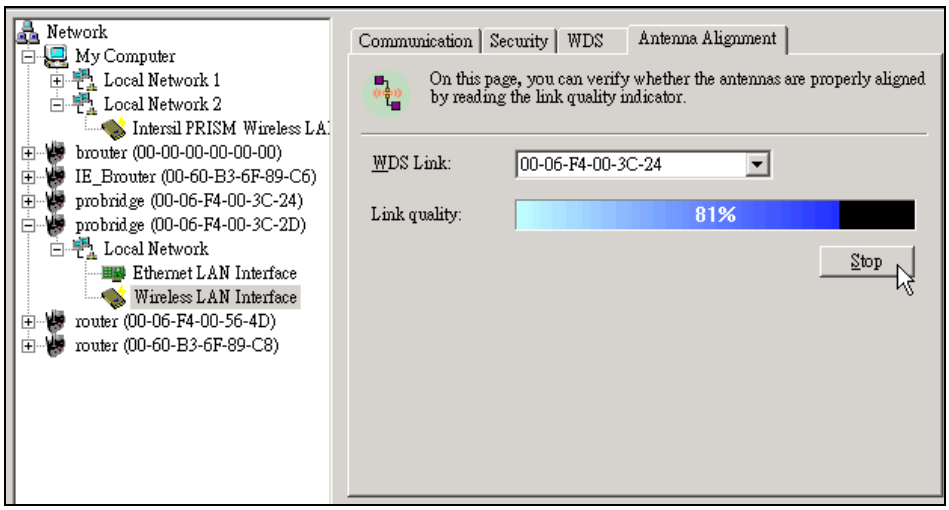


Fig. 38. Antenna alignment assistance.

Aligning external Antennas using PING:

To adjust the alignments of a pair of bridges' directional antennas:

1. Connect each bridge to a computer via Ethernet.
2. Configure the date rate of each bridge to the lowest value, 1Mbps.
3. Fix the alignment of the antenna on one side.
4. Adjust the alignment of the antenna on other side by using response time information obtained from PINGing (run PING.exe) the "fixed-side" computer.
5. Fine-tune the alignment of the antenna until you get a best response time.
6. Increase the data rate of each bridge simultaneously until a maximal workable data rate is reached. You may not be able to use the highest data rate, 11Mbps, because of the distance and the gain of the antennas.

Fig. 39 illustrates this idea.

Copyright 2005-2007 ValuePoint Networks, Inc. All rights reserved.

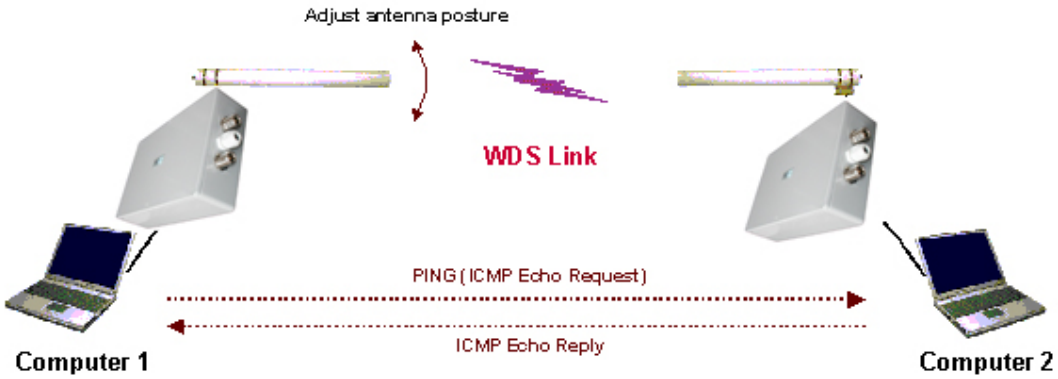


Fig. 39. Adjusting alignments of external directional antennas.

3.5.2. Security

IEEE 802.11 security settings include **SSID broadcasts**, **Wireless client isolation**, **Security mode**, **IEEE 802.11 Authentication algorithm**, **WEP keys**, and **MAC-Address-Based Access Control**.

3.5.2.1. Basic

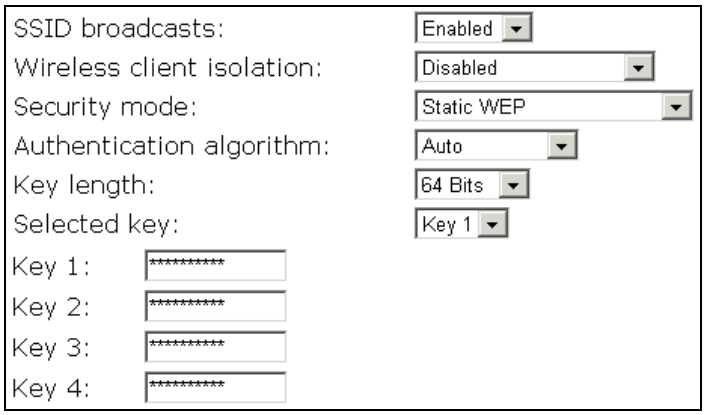


Fig. 40. Basic IEEE 802.11 security settings.

For security reasons, it's highly recommended that the security mode be set to options other than *Open System*. When the security mode is set to Open System, no authentication and data encryption will be performed. For additional security you can *disable* the SSID broadcasts functionality so that a wireless client computer with an "any" SSID cannot associate with the AP, and clients can not select the SSID from a list.

Wireless Client Isolation

When the **Wireless client isolation** setting is set to **This AP Only**, wireless clients of this AP as an AP cannot see each other, and wireless-to-wireless traffic is blocked. When the setting is set to **All APs in This Subnet**, traffic among wireless users of different APs in the same IP subnet is blocked. These behaviors are illustrated in the following diagrams.

Copyright 2005-2007 ValuePoint Networks, Inc. All rights reserved.

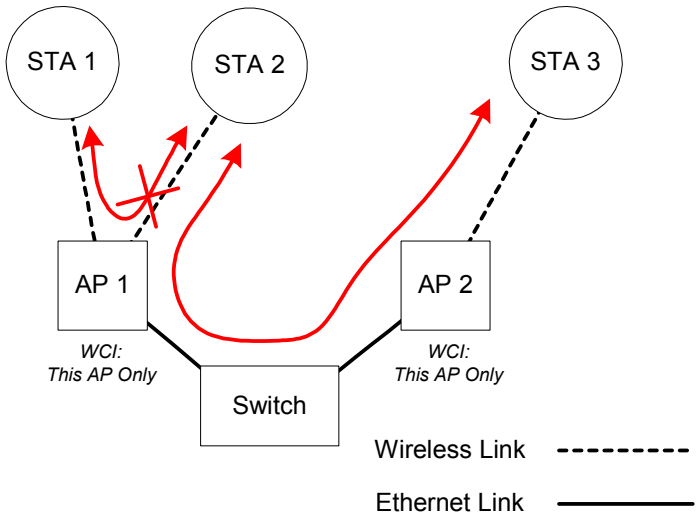


Diagram.A. Behavior of the “This AP Only” wireless client isolation option.

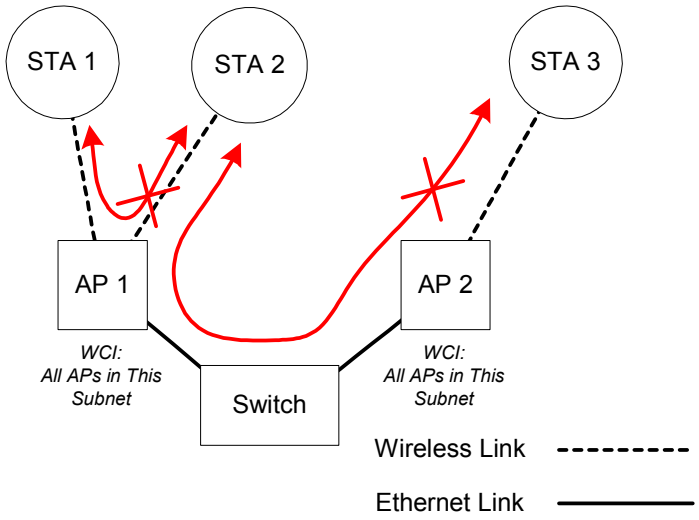


Diagram B. Behavior of the “All APs on This Subnet” wireless client isolation option.

As illustrated in Diagram A, when AP 1 and AP 2 are using the “This AP Only” option, wireless traffic between STA 1 and STA 2 is blocked by AP 1, while wireless traffic between STA 2 and STA 3, which are associated with different APs, is still allowed. If the “All APs in This Subnet” option is used as shown in Diagram B, AP 1 and AP 2 communicates with each other via an inter-AP protocol to share their STA association information and block wireless traffic among all the STAs.

Wireless Client Isolation is useful for WLANs deployed in public places. In this way, hackers have no chance to attack other wireless users in a *hotspot*.

Copyright 2005-2007 ValuePoint Networks, Inc. All rights reserved.

Security Modes

There are up to 7 security modes depending on AP model variations:

Basic SuperAP Modes:

- **Open System.** No authentication, no data encryption.
- **Static WEP.** WEP (Wired Equivalent Privacy) keys must be manually configured.

Additional Modes:

- **Static TKIP (WPA-PSK).** Only TKIP (Temporal Key Integrity Protocol) mechanism of WPA (Wi-Fi Protected Access) is enabled. In this mode, you have to specify the **Pre-shared key**, which will be used by the TKIP engine as a *master key* to generate keys that actually encrypt outgoing packets and decrypt incoming packets.

  NOTE: The number of characters of the **Pre-shared key** setting must be at least 8 and can be up to 63.

- **IEEE 802.1x EAP without Encryption (EAP-MD5).** The IEEE 802.1x functionality is enabled and the user-name/password-based EAP-MD5 authentication is used. No data encryption.
- **IEEE 802.1x EAP with Static WEP (EAP-MD5).** The IEEE 802.1x functionality is enabled and the user-name/password-based EAP-MD5 authentication is used. Data encryption is achieved by static WEP.
- **IEEE 802.1x EAP with Dynamic WEP (EAP-TLS, EAP-TTLS, PEAP).** The IEEE 802.1x functionality is enabled and dynamic WEP key distribution authentication (EAP-TLS, EAP-TTLS, or PEAP) is used. Data encryption is achieved by dynamic WEP.
- **IEEE 802.1x EAP with Dynamic TKIP (WPA).** This is a full WPA mode, in which both the TKIP and IEEE 802.1x dynamic key exchange mechanisms are enabled. The AP is highly secured in this mode.

See Section 3.5.3 for more information about IEEE 802.1x.

According to the IEEE 802.11 standard, WEP can be used for authentication and data encryption. Normally, *Shared Key* authentication is used if WEP data encryption is enabled. In rare cases, *Open System* authentication may be used when WEP data encryption is enabled. The **Authentication algorithm** setting is provided for better compatibility with wireless clients with various WLAN network adapters. There are three options available, including *Open System*, *Shared Key*, and *Auto*.

When WEP is enabled by a security mode, the **Key length** can be specified to be **64 Bits** or **128 Bits**. The **Selected key** setting specifies the key to be used as a *send-key* for encrypting traffic from the AP side to the wireless client side. All 4 WEP keys are used as *receive-keys* to decrypt traffic from the wireless client side to the AP side.

Copyright 2005-2007 ValuePoint Networks, Inc. All rights reserved.

LAN-to-LAN Bridge Interface (DR Only)

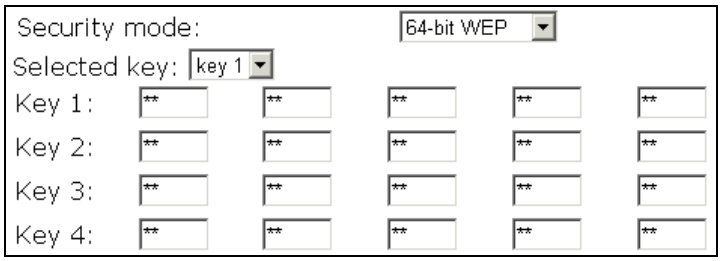


Fig. 41. IEEE 802.11 security settings for a LAN-to-LAN bridge interface.

Data transmitted over the Dual Radio bridge links in **AP Repeater** or **Bridge Repeater** mode can be encrypted by WEP (Wired Equivalent Privacy). Therefore, there are 3 security modes:

- **Open System.** No data encryption.
- **64-bit WEP.** Data encryption based on 64-bit WEP (Wired Equivalent Privacy).
- **128-bit WEP.** Data encryption based on 128-bit WEP (Wired Equivalent Privacy), and 128-bit keys are used.

NOTE: Each field of a WEP key setting is a *hex-decimal* number from 00 to FF. For example, when the security mode is **Static WEP** and the key length is **64 Bits**, you could set Key 1 to "00012E3ADF".

3.5.2.2. MAC-Address-Based Access Control

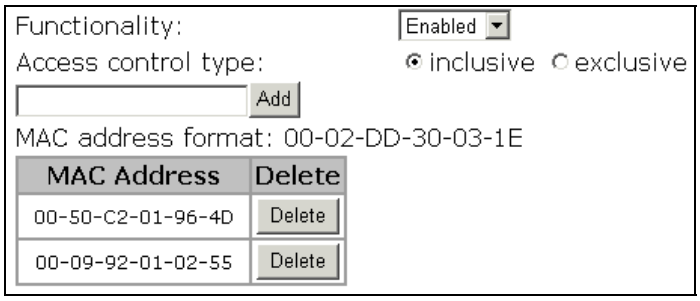


Fig. 42. MAC-address-based access control settings.

With **MAC-Address-Based Access Control**, you can specify the wireless client computers that are permitted or not permitted to associate with the AP. When the table type is set to *inclusive*, entries in the table are permitted to associate with the AP. When the table type is set to *exclusive*, entries in the table are not permitted to associate with the AP.

To *deny* wireless clients' access to the wireless network:

1. Select *Enabled* from the **Functionality** drop-down list.
2. Set the **Access control type** to *exclusive*.

Copyright 2005-2007 ValuePoint Networks, Inc. All rights reserved.

3. Specify the MAC address of a wireless client to be denied access, and then click **Add**.

4. Repeat Steps 3 for other wireless clients.

To *grant* wireless clients' access to the wireless network:

1. Select *Enabled* from the **Functionality** drop-down list.

2. Set the **Access control type** to *inclusive*.

3. Specify the MAC address of a wireless client to be denied access, and then click **Add**.

4. Repeat Steps 3 for other wireless clients.

To delete an entry in the access control table:

- Click **Delete** next to the entry.

NOTE: The maximum size of the access control table is 64 addresses.

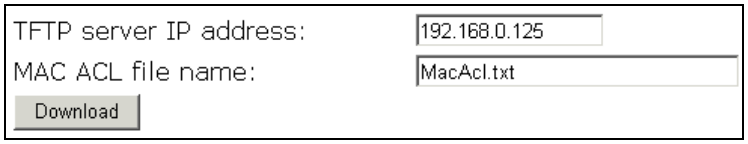


Fig. 43. MAC ACL download settings.

Instead of manually entering MAC addresses to the access control table one by one, you can prepare a text file that contains all the MAC addresses and put it on a TFTP server, and then command the AP to download the MAC ACL (Access Control List) file from the TFTP server. Fig. 44 shows the contents of a sample ACL file.

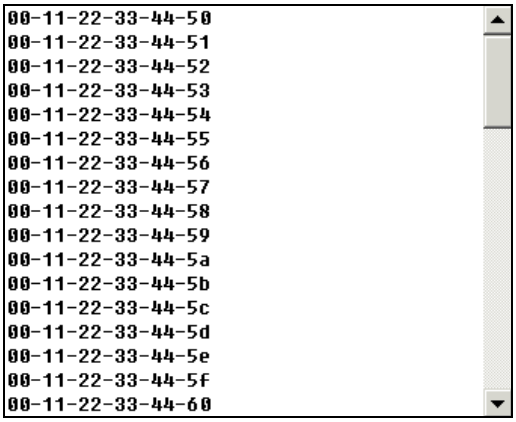


Fig. 44. Sample MAC ACL file.

To download a MAC ACL file from a TFTP server:

1. Specify the IP address of the TFTP server in the **TFTP server IP address** text box.

2. Specify the name of the MAC ACL file on the TFTP server in the **MAC ACL file name** text box.

Copyright 2005-2007 ValuePoint Networks, Inc. All rights reserved.

3. Click **Download**.

3.5.3. IEEE 802.1x/RADIUS (Adv+ and DR only)

IEEE 802.1x *Port-Based Network Access Control* is a new standard for solving some security issues associated with IEEE 802.11, such as lack of user-based authentication and dynamic encryption key distribution. With IEEE 802.1x and the help of a RADIUS (Remote Authentication Dial-In User Service) server and a user account database, an enterprise or ISP (Internet Service Provider) can manage its mobile users' access to its wireless LANs. Before granted access to a wireless LAN supporting IEEE 802.1x, a user has to issue his or her *user name* and *password* or *digital certificate* to the backend RADIUS server by EAPOL (Extensible Authentication Protocol Over LAN). The RADIUS server can record accounting information such as when a user logs on to the wireless LAN and logs off from the wireless LAN for monitoring or billing purposes.

The IEEE 802.1x functionality of the access point is controlled by the *security mode* (see Section 3.5.2.1). The wireless access point supports two authentication mechanisms—EAP-MD5 (Message Digest version 5) and EAP-TLS (Transport Layer Security). If EAP-MD5 is used, the user has to give his or her *user name* and *password* for authentication. If EAP-TLS is used, the wireless client computer automatically gives the user's *digital certificate* that is stored in the computer hard disk or a smart card for authentication. And after a successful EAP-TLS authentication, a session key is automatically generated for wireless packets encryption between the wireless client computer and its associated wireless access point. To sum up, EAP-MD5 supports only user authentication, while EAP-TLS supports user authentication as well as dynamic encryption key distribution.

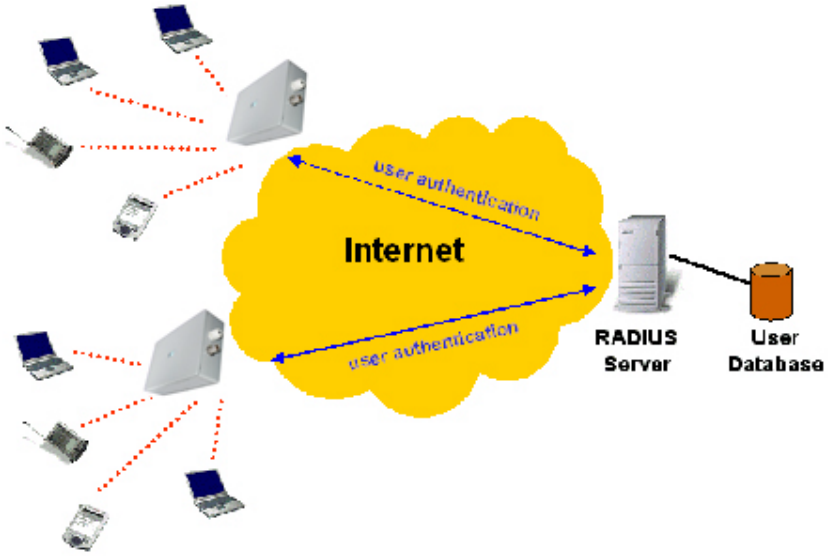


Fig. 45. IEEE 802.1x and RADIUS.

An access point supporting IEEE 802.1x can be configured to communicate with two RADIUS servers. When the primary RADIUS server fails to respond, the wireless access point will try to communicate with the secondary RADIUS server. You can specify the length of timeout and the number of retries before communicating with the *secondary* RADIUS server after failing to communicate with the primary RADIUS server.

An IEEE 802.1x-capable wireless access point and its RADIUS server(s) share a secret key so that they can authenticate each other. In addition to its IP address, a wireless access point can identify itself by an NAS (Network Access Server) identifier. The SuperAP sends the configured **host name** as the NAS ID. Each IEEE 802.1x-capable wireless access point must have a *unique* NAS identifier.

Copyright 2005-2007 ValuePoint Networks, Inc. All rights reserved.

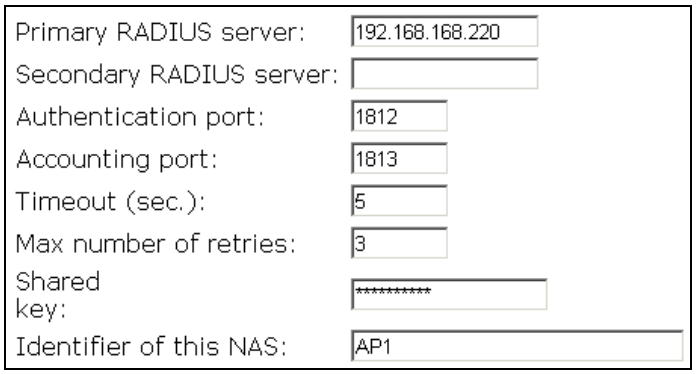


Fig. 46. IEEE 802.1x/RADIUS settings.

3.6. Configuring Advanced Settings

3.6.1. Packet Filters

The AP provides layer 2 (Ethernet Type Filters), layer 3 (IP Protocol Filters), and layer 4 (TCP/UDP Port Filters) filtering capabilities. The configuration processes for the filters are similar.

Functionality: whether this filtering capability is *enabled* or *disabled*.

Policy for matched packets: how a matched packet is processed—*discard* or *pass*.

To enable a filtering rule: select the check box to the left of the rule.

3.6.1.1. Ethernet Type Filters

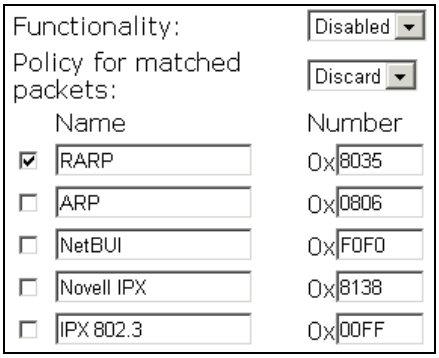


Fig. 47. Ethernet type filters settings.

The *Ethernet type* filed of the MAC (Media Access Control) header of a packet incoming from the WLAN or Ethernet interface is inspected for filtering. In a rule, specify the hex-decimal Ethernet type number and give the rule a name.

Copyright 2005-2007 ValuePoint Networks, Inc. All rights reserved.

3.6.1.2. IP Protocol Filters

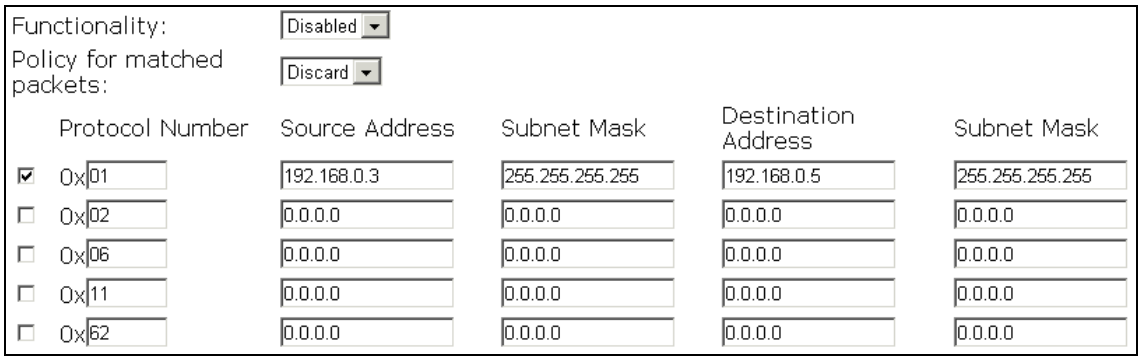


Fig. 48. IP protocol filters settings.

The protocol, source address, and destination address fields of a packet incoming from the WLAN or Ethernet interface is inspected for filtering. In a rule, specify the hex-decimal protocol number, source IP address range (Source IP Address AND Source Subnet Mask), and destination IP address range (Destination IP Address AND Destination Subnet Mask).

A source (destination) IP address range is determined by performing an AND operation on the source (destination) IP address field and the source (destination) subnet mask field. For example, if the source IP address field is 192.168.0.1 and the source subnet mask field is 255.255.255.0, the resultant source IP address range is 192.168.0.0 to 192.168.0.255.

TIP: ***Protocol Number*** is a field in IP packets. We have included some common IP protocols by default, but please see the pertinent IP RFCs for an up-to-date list of IP Protocols.

3.6.1.3. TCP/UDP Port Filters

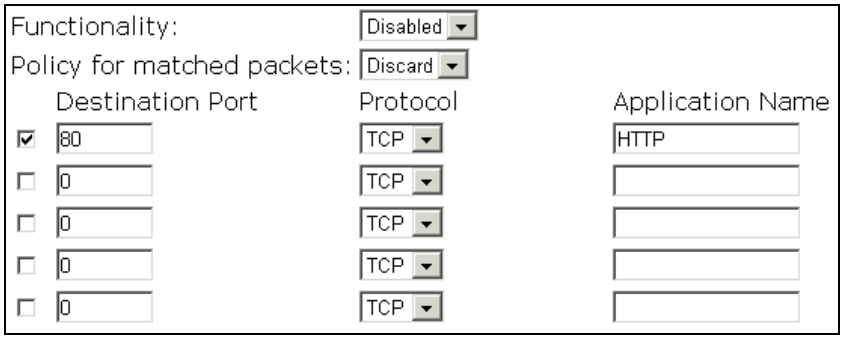


Fig. 49. TCP/UDP port filters settings.

The *destination port* field the TCP or UDP header of a packet incoming from the WLAN or Ethernet interface is inspected for filtering. To filter, specify the decimal **Destination Port**, **Protocol** type (TCP/UDP), and the name of the higher-level protocol (**Application Name**).

Copyright 2005-2007 ValuePoint Networks, Inc. All rights reserved.

3.6.2. Management

3.6.2.1. UPnP

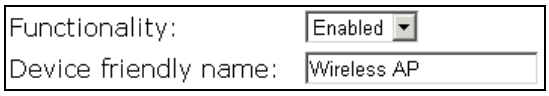


Fig. 50. UPnP settings.

UPnP (Universal Plug and Play) enables a Windows XP user to automatically discover peripheral devices and manage them via HTTP. When the UPnP functionality is enabled, you can see the AP in My Network Places of Windows XP. The AP can be given a *Device friendly name* that will be shown in My Network Places. *Double-clicking* the icon in My Network Places that stands for the AP will launch the default Web browser for you to configure the that AP.

3.6.2.2. System Log

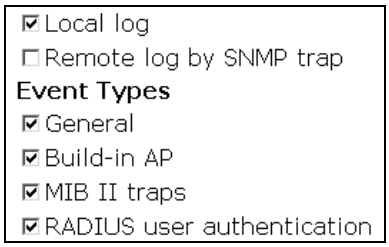


Fig. 51. System log settings.

System events can be logged to the on-board RAM of the AP (**Local log**) or sent to a remote computer on which an SNMP trap monitor program runs (**Remote log by SNMP trap**). See the next subsection for more information about SNMP trap settings.

The system events are divided into the following categories:

- **General**: system and network connectivity status changes.
- **Built-in AP**: wireless client association and WEP authentication status changes.
- **MIB II traps**: *Cold Start*, *Warm Start*, *Link Up*, *Link Down* and *SNMP Authentication Failure*.
- **RADIUS user authentication**: RADIUS user authentication status changes.

NOTE: The *SNMP Authentication Failure* trap is issued when using an incorrect community string to manage the AP via SNMP and the SNMP MIB II OID, **snmpEnableAuthenTraps**, is enabled (*disabled* by default).

Copyright 2005-2007 ValuePoint Networks, Inc. All rights reserved.

3.6.2.3. SNMP

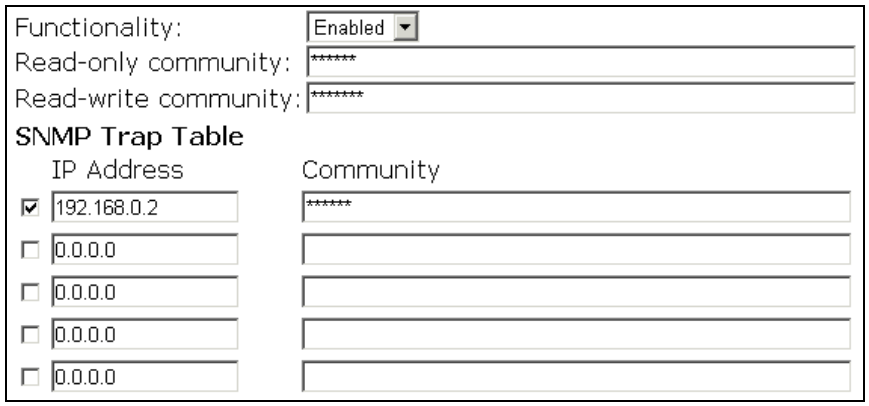


Fig. 52. SNMP settings.

The SNMP (Simple Network Management Protocol) functionality can be disabled, and you can specify the name (used as a *password*) of the read-only and read-write community. In addition, up to 5 SNMP trap targets can be set in the **SNMP Trap Table**.

To specify a trap target:

1. Type the IP address of the target host.
2. Type the **Community** for the host.
3. Select the corresponding check box next to the IP address text box.

Copyright 2005-2007 ValuePoint Networks, Inc. All rights reserved.

Appendix A: Default Settings

TIP: Press the **Default** (**SF-Reset**, or **Soft-Reset**) switch of a *powered-on* AP to reset the configuration settings to factory-default values.

Setting Name	Default Value
Global	
User Name	root
Password	root
IEEE 802.11	
Regulatory Domain	FCC (U.S.)
Channel Number	11
SSID	wireless
SSID Broadcasts	Enabled
Transmission Rate	Auto
Transmit Power	High
MAC Address	See the label on the accompanying PCMCIA card or the label on the housing of the AP.
Security Mode	Open System
Selected WEP Key	Key #1
WEP Key #1	00-00-00-00-00
WEP Key #2	00-00-00-00-00
WEP Key #3	00-00-00-00-00
WEP Key #4	00-00-00-00-00
MAC-Address-Based Access Control	Disabled
Access Control Table Type	Inclusive
Wireless Client Isolation	Disabled
AP Load balancing	Disabled
Link Integrity	Disabled
Association Control	
Max Number of Clients	64
Block Clients if Traffic Load Exceeds	Disabled
LAN Interface	
Method of obtaining an IP Address	Set manually
IP Address	192.168.0.1
Subnet Mask	255.255.255.0
Default Gateway	0.0.0.0
DHCP Server	Disabled
Management	
UPnP	Enabled
System Log	Local Log
SNMP	Enabled
SNMP read community	public
SNMP write community	private
Telnet	Enabled

Copyright 2005-2007 ValuePoint Networks, Inc. All rights reserved.

Appendix B: Troubleshooting

Check the following first:

- Make sure that the power of the AP is on and the Ethernet cables are connected firmly to the RJ-45 jacks of the AP.
- Make sure that the LED ALV of the AP is blinking to indicate the AP is working.
- Make sure the types of the Ethernet cables are correct. Recall that there are two types—*normal* and *crossover*.

B-1: Wireless Settings Problems

- **The wireless client computer cannot associate with an AP.**
  - Is the wireless client set in *infrastructure* mode?
    - Check the *operating mode* of the WLAN NIC.
  - Is the SSID of the WLAN NIC identical to that of the prospective AP?
    - Check the SSID setting of the WLAN NIC and of the AP.
  - Is the WEP functionality of the prospective AP enabled?
    - Make appropriate WEP settings of the client computer to match those of the AP.
  - Is the AP within range of wireless communication?
    - Check the *signal strength* and *link quality* sensed by the WLAN NIC.
  - Is the AP in Client or Bridge Repeater mode?
    - A WLAN NIC cannot associate with the AP in these modes.

Copyright 2005-2007 ValuePoint Networks, Inc. All rights reserved.

B-2: TCP/IP Settings Problems

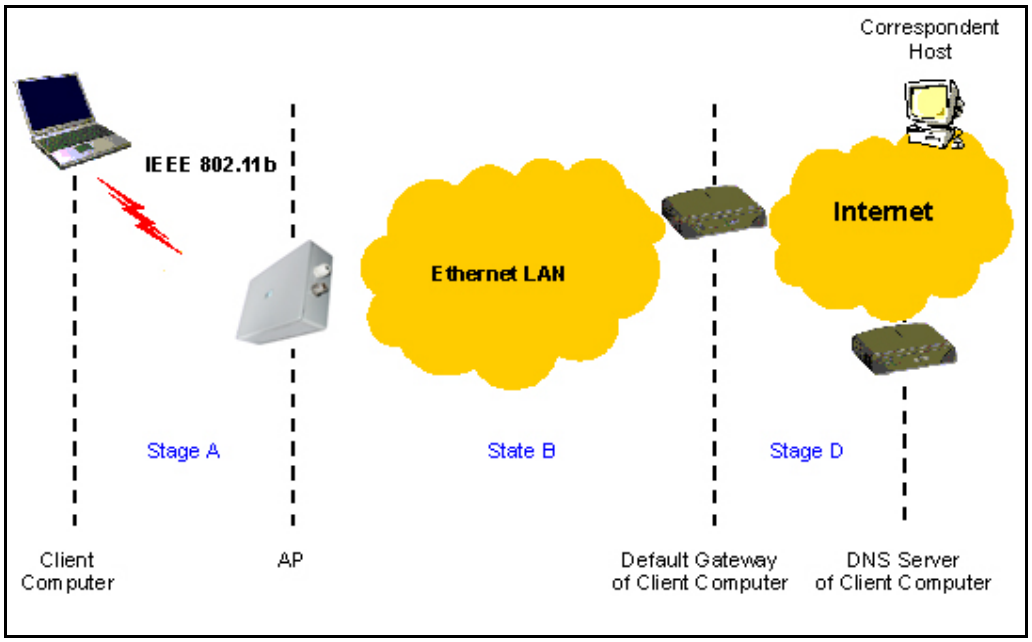


Fig. 53. Communication stages for a client to reach its correspondent host.

For a wireless client computer to communicate with a correspondent host on the Internet by the host's domain name (e.g. http://www.valuepointnet.com), it first sends a DNS request to a DNS server on the Internet. The DNS request travels first to the AP, then the AP relays this request to the default gateway of the client computer. Finally, this request is forwarded by the gateway to the DNS server on the Internet. The DNS reply issued by the DNS server is transmitted back to the client computer following a reverse path. When the client computer receives the DNS reply, it knows the IP address of the correspondent host and sends further packets to this IP address.

As illustrated in Fig. 53, the communication path could be broken at some of the stages. The OS-provided network diagnostic tool, **ping.exe**, can be employed to find out TCP/IP-related communication problems.

NOTE: If *two or more* NICs are installed and operating on a client computer, TCP/IP may not work properly due to incorrect entries in the routing table. Use the OS-provided command-line network tool, **route.exe**, to add or delete entries from the routing table. Or, use Windows-provided **Device Manager** to disable unnecessary NICs.

Solve the following problems in order:

- **The AP does not respond to *ping* from the client computer.**
  - Are two or more NICs installed on the client computer?
    - Use the OS-provided command-line network tool, **route.exe**, to modify the contents of the routing table.
    - Use Windows-provided **Device Manager** to disable unnecessary NICs.
  - Is the underlying link (Ethernet or IEEE 802.11) established?

Copyright 2005-2007 ValuePoint Networks, Inc. All rights reserved.

- Make sure the Ethernet link is OK.
- Make sure the wireless settings of the wireless client computer and of the AP match.

- Is Wireless Client or Layer-two isolation enabled on the default gateway, or an intervening AP?
  - Disable Isolation features to access local APs or other hardware on the LAN.
- Are the IP address of the *client computer* and the IP address of the *AP* in the same IP subnet?
  - Use **WinIPCfg.exe** or **IPConfig.exe** to see the current IP address of the client computer. Make sure the IP address of the client computer and the IP address of the AP are in the same IP subnet.

TIP: If you forget the current IP address of the AP, use Wireless Router/AP Browser to get the information (see Appendix B-3).

- **The default gateway of the client computer does not respond to *ping* from the client computer.**
  - Solve the preceding problem first.
  - Are the IP address of the *AP* and the IP address of the *client computer* in the same IP subnet?
  - If you cannot find any incorrect settings of the AP, the default gateway may be really down or there are other communication problems on the network backbone.
- **The DNS server(s) of the client computer do not respond to *ping* from the client computer.**
  - Solve the preceding problems first.
  - If you cannot find any incorrect settings of the AP, the default gateway of the AP may be really down or there are other communication problems on the network backbone.

B-3: Other Problems

- **The AP has been set to obtain an IP address automatically by DHCP. How can I know its acquired IP address so that I can manage it using a Web browser?**
  - If you have access to the DHCP Server, check its client list for the address assigned to the AP.
  - Use the Wireless Network Manager. This utility can discover nearby APs and show their MAC addresses, IP addresses, and other settings. You must be on the correct subnet to access the AP this way.
- **The AP stops working and does not respond.**

Copyright 2005-2007 ValuePoint Networks, Inc. All rights reserved.

- Reset the AP to Factory Default settings.
- The firmware of the AP may be stuck in an incorrect state.
  - Unplug the power connector from the power jack, and then re-plug the connector to restart the AP.
  - Contact our technical support representatives to report this problem, so that the bugs can be static in future firmware versions.
- If the AP still does not work after restarting, there may be hardware component failures in the AP.
  - Contact our technical support representatives for repair.

- **The AP is working, but I cannot access the Web Management interface.**
  - Your browser may have a bad HTML page in the cache.
    - Hold down CTRL and click 'Refresh' button on the browser to force the page to load
    - Delete the contents of the web cache under Tools – Internet Options – Temporary Internet Files – Delete Files
  - Manage the AP via Telnet (Not available on DR)
  - Manage the AP via Wireless Network Manager

B-3: Contacting Technical Support

Please contact us at support@valuepointnet.com

Copyright 2005-2007 ValuePoint Networks, Inc. All rights reserved.

Appendix C: Additional Information

C-1: Distances and Data Rates for Clients

Important Notice: Maximum distances posted below are actual tested distance thresholds. However, there are many variables such as barrier composition and construction and local environmental interference that may impact your actual distances and cause you to experience distance thresholds far lower than those we post below.

IEEE 802.11 Maximum Distance Table				
Environmental Condition	**Speed and Distance Ranges**			
	11 Mbps	5.5 Mbps	2 Mbps	1 Mbps
Open Environment: A "line-of-sight" environment with no interference or obstructions between Access Point and Users.	160 m (524 ft)	270 m (886 ft)	400 m (1312 ft)	457 m (1500 ft)
Semi-Open Environment: An environment with no major obstructions such as walls or privacy cubicles between Access Point and users.	50 m (164 ft)	70 m (230 ft)	90 m (295 ft)	120 m (394 ft)
Closed Environment: A typical office or home environment with floor to ceiling obstructions between Access Point and users.	25 m (82 ft)	35 m (115 ft)	45 m (148 ft)	55 m (180 ft)

NOTE: Distances are limited by Client (35-50mW) receiver. Far greater distances are achieved using WDS and directional antennas between APs.